

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-094549

(43)Date of publication of application : 06.04.2001

(51)Int.Cl.

H04L 9/08

G06F 12/14

G06F 15/00

G09C 1/00

G11B 20/10

H04L 9/32

(21)Application number : 11-309721

(71)Applicant : SONY CORP

(22)Date of filing : 17.09.1999

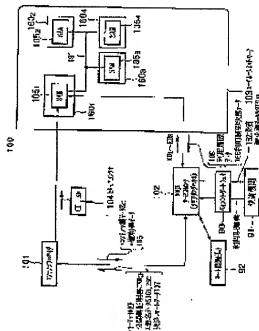
(72)Inventor : NONAKA SATOSHI
EZAKI TADASHI

(54) DATA PROVIDING SYSTEM AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data providing system which can protect the profit of persons concerned in a data providing device.

SOLUTION: An EMD service center 102 generates a stored key file KF by ciphering title deed data 106 and content key data Kc that a content provider 101 generates with key data for distribution and sends the file to a content provider 101. The content provider 101 supply a secure container 104 including a content file CF containing the content data C deciphered by using the content key data Kc and the key file KF received from the EMD service center 102 to SAM 105, etc., of a user home network 103.



【特許請求の範囲】

【請求項1】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項2】前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを前記キーファイルに付加する請求項1に記載のデータ提供システム。

【請求項3】前記データ提供装置は、前記コンテンツデータを格納したコンテンツファイルを作成し、当該コンテンツファイルを前記データ処理装置に提供する請求項1に記載のデータ提供システム。

【請求項4】前記データ提供装置は、前記コンテンツファイルの作成者の正当性を検証するための署名データを前記コンテンツファイルに付加する請求項3に記載のデータ提供システム。

【請求項5】前記データ提供装置は、前記権利書データを作成して前記管理装置に送り、

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う請求項1に記載のデータ提供システム。

【請求項6】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュール

ルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項7】前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する請求項6に記載のデータ提供システム。

【請求項8】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する請求項6に記載のデータ提供システム。

【請求項9】前記データ提供装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記モジュールを前記データ処理装置に配給する請求項7に記載のデータ提供システム。

【請求項10】前記データ処理装置は、前記モジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者との、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する請求項9に記載のデータ提供システム。

【請求項11】前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する請求項6に記載のデータ提供システム。

【請求項12】前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる請求項11に記載のデータ提供システム。

【請求項13】前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項10に記載のデータ提供システム。

【請求項14】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納

1

データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項18】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配送し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項19】 データ提供装置からデータ処理装置にコンテンツデータを転送し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に記録し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 20】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 21】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 22】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 23】前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する請求項 2 に記載のデータ提供システム。

【請求項 24】前記データ配給装置は、前記提供を受け

た第 1 のモジュールを包括させた前記第 2 のモジュールを作成し、当該作成した第 2 のモジュールを前記データ処理装置に配給する請求項 22 に記載のデータ提供システム。

【請求項 25】前記データ配給装置は、前記コンテンツデータの価格を示す価格データをさらに格納した前記第 2 のモジュールを前記データ処理装置に配給する請求項 22 に記載のデータ提供システム。

【請求項 26】前記データ配給装置は、前記データ提供装置が前記コンテンツデータについて決定した卸売価格に基づいて、前記価格データを決定する請求項 25 に記載のデータ提供システム。

【請求項 27】前記データ提供装置は、前記コンテンツ鍵データ、前記コンテンツ鍵データおよび前記権利書データのうちの少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第 1 のモジュールを前記データ配給装置に提供する請求項 22 に記載のデータ提供システム。

【請求項 28】前記データ配給装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうちの少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第 2 のモジュールを前記データ処理装置に提供する請求項 22 に記載のデータ提供システム。

【請求項 29】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前期購入および前期利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う請求項 22 に記載のデータ提供システム。

【請求項 30】前記データ処理装置は、前記データ配給装置の前記配給に関しての配給利用履歴データを前記データ配給装置に送信し、前記データ配給装置は、前記配給利用履歴データに基づいて、前記配給に関しての課金処理を行う請求項 22 に記載のデータ提供システム。

【請求項 31】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前

記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 3 2】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、前記受信した前記コンテンツ鍵データおよび前記権利書データを登録する請求項 3 1 に記載のデータ提供システム。

【請求項 3 3】前記データ提供装置は、前記コンテンツファイルの作成者および提供者と、前記キーファイルの提供者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第 1 のモジュールを前記データ処理装置に配給する請求項 3 1 に記載のデータ提供システム。

【請求項 3 4】前記データ配給装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第 2 のモジュールを前記データ処理装置に配給する請求項 3 1 に記載のデータ提供システム。

【請求項 3 5】前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項 3 3 に記載のデータ提供システム。

【請求項 3 6】前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データとをさらに格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項 3 3 に記載のデータ提供システム。

【請求項 3 7】前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装

置に配給する前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項 3 6 に記載のデータ提供システム。

【請求項 3 8】前記データ配給装置は、自らの秘密鍵データを用いて前記署名データを作成し、前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項 3 3 に記載のデータ提供システム。

【請求項 3 9】前記データ配給装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項 3 8 に記載のデータ提供システム。

【請求項 4 0】前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項 3 8 に記載のデータ提供システム。

【請求項 4 1】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一つを決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う請求項 3 1 に記載のデータ提供システム。

【請求項 4 2】前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第 2 のモジュールを前記データ処理装置に配給する請求項 3 1 に記載のデータ提供システム。

【請求項 4 3】前記管理装置は、前記データ配給装置から受けた前記価格データを登録する請求項 4 2 に記載のデータ提供システム。

【請求項 4 4】前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータの、外部から監視および改竄困難なモジュールを有する請求項 3 1 に記載のデータ提供システム。

【請求項 4 5】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

9

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキープファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項46】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キープファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キープファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キープファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項47】前記コンテンツファイルおよび前記キープファイルには、相互の対応関係を明示するためのデータが含まれる請求項46に記載のデータ提供システム。

【請求項48】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、当該作成したキープファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用い

10

て暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キープファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

10

【請求項49】前記コンテンツファイルおよび前記キープファイルには、相互の対応関係を明示するためのデータが含まれる請求項48に記載のデータ提供システム。

【請求項50】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キープファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キープファイルを格納した第2のモジュールを前記データ処理装置に配給し、

30

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項51】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キープファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記キープファイルとを個別に前記データ配給装置

50

に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 5 2】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 5 3】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 5 4】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前

記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 5 5】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 5 6】前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第 1 のモジュールを作成し、当該第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第 1 のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを生成し、当該第 2 のモジュールを前記データ処理装置に配給する請求項 5 に記載のデータ提供システム。

【請求項 5 7】前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利

害データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する請求項5に記載のデータ提供システム。

【請求項58】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化したコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項59】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納され

たコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項60】前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する請求項59に記載のデータ提供システム。

【請求項61】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項62】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

15 前記データ処理装置は、前記基給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記基給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 63】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 64】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供シ

ステム。

【請求項 65】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

10 前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

20 前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 66】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

40 前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 67】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処

17

理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイル

を作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 68】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツ鍵データを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 69】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

18

前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 70】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 71】データ提供装置からデータ処理装置にコ

ンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 72】 データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利表データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 73】 データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、略号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す略号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルを含むコンテンツファイルを格納したモジュールを前記データ処理装置に配送し、前記データ処理装置において、前記暗号化を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利管理データを復号し、当該復号した権利管理データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 74】 データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提

他方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 75】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利管理データを復号し、当該復号した権利管理データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項76】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配送し、

前記データ処理装置において、前記登録を受けた前記モジュールに格納された前記コンテンツ識別データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

21

【請求項 7】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 7】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 7】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

22

【請求項 8】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 8】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 8】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを、前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 2 のモジュールを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項83】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項84】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、

前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ

提供方法。

【請求項85】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項86】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項87】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

25

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、
前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱

【請求項8】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱

【請求項9】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当

26

該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項10】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項11】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項12】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給

装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 93】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 94】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受

けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 95】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 96】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づ

【請求項 101】複数のデータ提供装置、データ配給装

置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 102】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方

法。

【請求項 103】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツデータを提供するデータ提供システムおよびその方法に関する。

【0002】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザーのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このようなデータ提供システムの一つに、音楽データを配信する従来の EMD (Electronic Music Distribution : 電子音楽配信) システムがある。

【0003】図 145 は、従来の EMD システム 700 の構成図である。図 145 に示す EMD システム 700 では、コンテンツプロバイダ 701a、701b が、サブスクリプション 710 に対し、コンテンツデータ 704a、704b、704c と、著作権情報 705a、705b、705c とを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報 705a、705b、705c には、例えば、SCMS

(Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツ鍵データ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報にコンテンツ鍵データ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA (Conditional Access) モジュール711に送信する。

【0005】CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービス

プロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益配分を行う。このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】【発明が解決しようとする課題】ところで、SCMSは、コンテンツデータを例えば2世代以上のわたって複製することを禁止するものであり、1世代の複製は無駄に行うことができ、著作権者の保護として不十分であるという問題がある。

【0009】また、上述したEMDシステム700では、サービスプロバイダ710が暗号化していないコンテンツデータを技術的には自由に転換するため、コンテンツプロバイダ701の関係者はサービスプロバイダ710の行為等を監視する必要があり、当該監視の負担が大いと共に、コンテンツプロバイダ701の利益が不当に損なわれる可能性が高いという問題がある。また、上述したEMDシステム700では、ユーザの端末装置709がサービスプロバイダ710から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ701の利益が不当に損なわれるという問題がある。

【0010】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法を提供することを目的とする。また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法を提供することを目的とする。

【0011】【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第1の観点のデータ提供システムは、好ましくは、デー

タ提供装置からデータ処理装置にコンテンツデータを転送し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを復号し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを用いて、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0012】本発明の第1の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0013】また、本発明の第2の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0014】本発明の第2の観点のデータ提供システムの作用は以下に示すようになる。管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。そして、当該作成されたキーファイルが、前記管理装置から前記データ提供装置に配給される。そして、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイル

とを格納したモジュールが、前記データ提供装置から前記データ処理装置に配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0015】本発明の第3の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0016】本発明の第3の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0017】また、本発明の第4の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

37

て、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0018】本発明の第4の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルとが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【0019】また、本発明の第5の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0020】本発明の第5の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【0021】また、本発明の第6の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテ

38

ンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0022】また、本発明の第6の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0023】また、本発明の第7の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0024】本発明の第7の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管

理装置から受けた前記キーファイルとが個別に配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

【0025】また、本発明の第8の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0026】本発明の第8の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【0027】また、本発明の第9の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0028】本発明の第9の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが個別に配給される。そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【0029】また、本発明の第10の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0030】本発明の第10の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【0031】また、本発明の第11の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前

41

記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0032】本発明の第11の観点のデータ提供システムの作用は以下に示ようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。そして、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータが配給される。そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

【0033】また、本発明の第12の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0034】本発明の第12の観点のデータ提供システムの作用は以下に示ようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールが提供され

42

る。そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号され、当該復号された権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

10 【0035】また、本発明の第13の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

30 【0036】また、本発明の第14の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

44

10

20

40

10

20

30

50

16

【 0 0 4 4 】、本発明の第 2 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスターデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、データ提供されたマスターステータスをコンテンツ鍵データを用いて暗号化したコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルと前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルは前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイル

【0047】また、本発明の第25の視点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテ

47

ツプファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ供給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に供給し、前記データ処理装置は、前記供給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記暗号化を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４８】また、本発明の第２６の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利客データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利客データを復号し、当該復号した権利客データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0049】また、本発明の第2の視点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り回しを示す暗号データと、前記暗号データとを格納したキープファイルを作成し、当該作成したキープファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データテーブル装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記コンテンツファイルに格納された前記コンテンツ鍵データおよび前記暗号化データを

48

復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 5 0 】 また、本発明の第 2 8 の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複読の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 5 1 】 また、本発明の第 2 9 の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５２】また、本発明の第３０の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提

供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化されたコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0053】また、本発明の第31の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化されたコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0054】また、本発明の第32の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化されたコンテンツデータを格納したコンテンツフ

イルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0055】また、本発明の第33の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化されたコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0056】また、本発明の第1の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当

51

該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0057】 本発明の第2の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツデータと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツデータを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツデータおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【10058】本発明の第3の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したミニョールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記ミニョールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0059】また、本発明の第4の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利害データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利害データを復号し、当該復号し

52

た権利者データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 6 0 】 また、本発明の第5の視点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いはコンテンツ番号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0061】また、本発明の第6の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配信し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツデータと前記コンテンツデータの取り扱いは示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツデータを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配信し、前記データ処理装置において、前記配信を受けた前記モジュールに格納された前記コンテンツデータおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【10062】た、本発明の第7の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを供給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いは必ずしも暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に供給し、前記データ処理装置において、前記処理装置を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記処理装置を受けたコンテンツデータの取り扱いを決定する。

53

【0063】また、本発明の第8の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルの前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0064】また、本発明の第9の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0065】また、本発明の第10の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データに基づいて、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0066】また、本発明の第11の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供システムであって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化

54

された権利書データとを格納したキーファイルを作成し、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0067】また、本発明の第12の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルの前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0068】また、本発明の第13の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復

号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0069】また、本発明の第14の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツ鍵データの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ配給装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0070】また、本発明の第15の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0071】また、本発明の第16の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管

理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0072】また、本発明の第17の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0073】また、本発明の第18の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記

コンテンツデータの取り扱いを決定する。

【0074】また、本発明の第19の観点のデータ提供方法は、データ提供装置からデータ供給装置にコンテンツデータを提供し、前記データ供給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ供給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ供給装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ供給装置に配給し、前記データ供給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ供給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0075】また、本発明の第20の観点のデータ提供方法は、データ提供装置からデータ供給装置にコンテンツデータを提供し、前記データ供給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ供給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ供給装置に提供し、前記データ供給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0076】また、本発明の第21の観点のデータ提供方法は、データ提供装置、データ供給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスターソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ供給装置および前記データ処理装置を管理し、前記提供されたマスターソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化さ

れた権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ供給装置に提供し、前記データ供給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0077】また、本発明の第22の観点のデータ提供方法は、データ提供装置、データ供給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスターソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ供給装置および前記データ処理装置を管理し、前記提供されたマスターソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ供給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ供給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0078】また、本発明の第23の観点のデータ提供方法は、データ提供装置、データ供給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ供給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ供給装置に提供し、前記データ供給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り

59

扱いを決定する。

【0079】また、本発明の第24の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキープファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキープファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キープファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 8 0 】 また、本発明の第 2 5 の観点のデータの提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 8 1 1 】 た、本発明の第 2 6 の視点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ離データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ離データと、前記コンテンツデータの

取り扱いは示す略号化された権利書データとを格納した
キーファイルを作成し、当該作成したキーファイルを前
記データ配給装置に提供し、前記データ配給装置は、前
記データベース装置から得た前記コンテンツファイルと
、前記データ配給装置から提供を受けたキーファイルと
を前記データ処理装置に配給し、前記データ処理装置
は、前記配給を受けた前記キーファイルに格納された前
記コンテンツ鍵データおよび前記権利書データを復号
し、当該復号した権利書データに基づいて、前記配給を
10 受けたコンテンツファイルに格納されたコンテンツデ
ータの取り扱いを決定する。

【００８２】また、本発明の第２の観点のデータ提供方法は、データ提供装置、データ処理装置、管理装置、データベース装置およびデータ配給装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いは示す暗号化された権利付データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利付データを復号し、当該復号した権利付データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いは決定する。

【0083】また、本発明の第2の観点のデータの提供方法は、複数のデータ提供装置、データ配給装置、帳簿の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータを用いてコンテンツデータを暗号化し、当該暗号化されたコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツデータと、前記コンテンツデータの取り扱いを示す暗号化された権利データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に供給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツデータおよび前記権利データを復号し、当該復号した権利データに基づいて、前記権利

61

を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0084】また、本発明の第29の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルの前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0085】また、本発明の第30の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルの前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ配給装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0086】また、本発明の第31の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納

62

し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0087】また、本発明の第32の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルと前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ配給装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0088】また、本発明の第33の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターズを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターズ

スをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0089】

【発明の実施の形態】以下、本発明の実施形態に係わるEMD (Electronic Music Distribution: 電子音楽配信) システムについて説明する。

第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。本実施形態において、ユーザに配信されるコンテンツ (Content) データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ (クリアリング・ハウス、以下、ESCとも記す) 102およびユーザホームネットワーク103を有する。ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105、105aが、それぞれ請求項1および請求項6などに係るデータ提供装置、管理装置およびデータ処理装置に対応している。まず、EMDシステム100の概要について説明する。EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データKc、コンテンツデータCの使用許諾条件などの権利内容を示す権利書 (UCP: Usage Control Policy) データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある接続装置であるEMDサービスセンタ102に送る。

【0090】EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データKc、権利書データ106並びに電子透かし情報管理データを登録 (認証および権限化) する。また、EMDサービスセンタ102は、対応する期間の配信用鍵データKD1~KD5で暗号化したコンテンツ鍵データKc、権

利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

【0091】また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテンツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ (本発明のモジュール) 104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0092】ユーザホームネットワーク103は、例えば、ネットワーク機器1601およびAV機器1602~1604を有する。ネットワーク機器1601は、SAM (Secure Application Module) 1051を内蔵している。AV機器1602~1604は、それぞれSAM1052~1054を内蔵している。SAM1051~1054相互間は、例えば、IEEE (Institute of Electrical and Electronics Engineers) 1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0093】SAM1051~1054は、ネットワーク機器1601がコンテンツプロバイダ101からネットワークなどを介してオフラインで受信したセキュアコンテナ104、および/または、コンテンツプロバイダ101からAV機器1602~1604に記録媒体を介してオフラインで供給されたセキュアコンテナ104に対応する期間の配信用鍵データKD1~KD5を用いて復号した後に、署名データの検証を行う。SAM1051~1054に供給されたセキュアコンテナ104は、ネットワーク機器1601およびAV機器1602~1604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM1051~1054は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴 (Usage Log) データ108として記録すると共に、購入形態を示す利用制御状態データ166を作成する。利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。利用制御状態データ166は、例えば、購入形態が

65

決定される度に、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0094】EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を設定（計算）し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0095】本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての（ルート認証局92の下層に位置する）セカンド認証局（Second Certificate Authority）としての役割を果たし、コンテンツプロバイダ101およびSAM1051~1054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化すること、EMDサービスセンタ102の認証機能の一つである。また、EMDサービスセンタ102は、例えば、配信用鍵データKD1~KDnなどの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP（Suggested Retailer Price）とSAM1051~SAM1054から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理（利益分配）機能を有する。

【0096】図2は、セキュアコンテナ104の概念をまとめた図である。図2に示すように、セキュアコンテナ104には、コンテンツプロバイダ101が作成したコンテンツファイルCFと、EMDサービスセンタ102が作成したキーファイルKFとが格納されている。コンテンツファイルCFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、コンテンツ鍵データKcを用いた暗号化されたコンテンツデータCと、これらについてのコンテンツプロバイダ101の秘密鍵データKcp、sを用いた署名データとが格納されている。キーファイルKFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、配信用鍵データKD1~KDnによ

66

って暗号化されたコンテンツ鍵データKcおよび権利書データ106と、これらについてのEMDサービスセンタ102の秘密鍵データKcp、sによる署名データとが格納されている。

【0097】以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

【コンテンツプロバイダ101】図3は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM1051~1054との間で送受信されるデータに関連するデータの流れが示されている。また、図4には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。なお、図4以降の図面では、署名データ処理部、および、セッション鍵データKssを用いた暗号化・復号部に入出力するデータの流れは省略している。

【0098】図3および図4に示すように、コンテンツプロバイダ101は、コンテンツマスターソースデータベース111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、伸長部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、キーファイルデータベース118b、記憶部（データベース）119、相互認証部120、暗号化・復号部121、権利書データ作成部122、暗号検査部123、SAM管理部124、EMDサービスセンタ管理部125およびコンテンツID生成部850を有する。コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでEMDサービスセンタ102に登録し、自らの識別子（識別番号）CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受け、図3および図4に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

【0099】コンテンツマスターソースデータベース111は、ユーザホームネットワーク103に提供するコンテンツのマスターソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

【0100】電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報（Source Watermark）Ws、コピー管理用電子透かし情報（Copy Control Watermark）Wc、ユーザ電子透かし情報（User Watermark）Wuおよびリンク用電子透かし情報（Link Watermark）WLなどを埋め込んでコンテンツデータS112を生成し、コンテンツデ

ークS112を圧縮部113に出力する。

【0101】ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリングID付、オーサリング機器ID (Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Wcは、アナログインタフェース経出でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテンツ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM1051~1054の識別子SAM_ID1~SAM_ID4が含まれる。リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配給された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなわち、当該コンテンツデータCの受信先において、電子透かし情報デコダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

【0102】具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD (Mini Disk) などの光ディスクなどの可搬メディアに搭載されているメディアSAMに記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテ

ンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【0103】なお、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ302は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

【0104】また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器1601およびAV機器1602~1604が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク103では、EMDサービスセンタ102が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断すること、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0105】圧縮部113は、コンテンツデータS112を、例えば、ATRAC3 (Adaptive Transform Acoustic Coding) (商標) などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。この場合に、圧縮部113による圧縮時に、コンテンツデータに対しての電子透かし情報の埋め込みを再び行ってもよい。具体的には、図3に示すように、伸長部116においてコンテンツデータ113を伸長してコンテンツデータS116を生成し、聴感検弁部123においてコンテンツデータS116を再生したときに、電子透かし情報の埋め込みが音質に与える影響を、例えば聴感に人間が聴いて判断し、所定の基準を満たさない場合には、電子透かし情報付加部112に電子透かし情報の埋め込み処理を再び行うように指示する。これにより、例えば、データの損失を伴う音声圧縮方式を採用したときに、当該圧縮によって、埋め込んだ電子透かし情報が落ちてしまった場合に適切に対処できる。また、圧縮したコンテンツデータを再度伸長して、埋め込みを行った電子透かし情報を正確に検出できるか否かの確認を行ってもよい。この場合に、音質聴感の検証も行い、聴感上問題がある場合には、電子透かし情報の埋め込みの調整を

行う。例えば、マスキング効果を利用して電子透かし情報を埋め込む場合には、電子透かし情報の埋め込みを行うレベルを調整する。

【0106】暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS13を暗号化してコンテンツデータCを生成し、これをセキュアコンテンツ作成部118に出力する。また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/V伸長用ソフトウェアSoft、メタデータMetaおよび電子透かし情報管理データWMを暗号化した後に、セキュアコンテンツ作成部117に出力する。

【0107】DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号化方式である。DESの処理は、平文を複写し、暗号文に変換する部分(データ複写部)と、データ複写部で使用する鍵(拡大鍵)データを共通鍵データから生成する部分(鍵処理部)とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ複写部の基本的な処理を簡単に説明する。

【0108】まず、平文の64ビットは、上位32ビットのH₀と下位32ビットのL₀とに分割される。鍵処理部から供給された48ビットの拡大鍵データK₀および下位32ビットのL₀を入力とし、下位32ビットのL₀を複写したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH₀と、F関数の出力との排他的論理和が算出され、その結果はL₁とされる。また、L₀は、H₁とされる。そして、上位32ビットのH₀および下位32ビットのL₀を基に、以上の処理を16回繰り返して、得られた上位32ビットのH₁₆および下位32ビットのL₁₆が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【0109】乱数発生部115は、所定ビット数の乱数を生じ、当該乱数をコンテンツ鍵データKcとして記憶部119に記憶する。なお、コンテンツ鍵データKcは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテンツプロバイダ101によって固有のコンテンツ鍵データKcを用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データKcを用いてもよい。

【0110】キーファイルデータベース118bには、図4に示すように、EMDサービスセンタ管理部125を介してEMDサービスセンタ102から受信した図5

(B)に示すキーファイルKFが記憶される。キーファイルKFは、コンテンツデータC内に存在し、後述するように、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSDによって、対応するコンテンツファイルCFとの間でリンク関係が指定されている。キーファイルKFには、図5(B)および図7に示すように、ヘッダ、コンテンツ鍵データKc、権利書データ(使用許諾条件)106、SAMプログラム・ダウンロード・コンテンツSDC1~SDC3および署名データS1GK1、ESCが格納されている。ここで、コンテンツプロバイダ101の秘密鍵データKESC、sを用いた署名データは、図5(B)に示すようにキーファイルKFに格納される全てのデータに対しての署名データK1、ESCにしてもよいし、図7に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データKcおよび権利書データ106に対しての署名データと、SAMプログラム・ダウンロード・コンテンツSDC1~SDC3に対しての署名データとを別々に設けてもよい。コンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテンツSDC1~SDC3とは、それぞれ対応する順位の配信用鍵データKD1~KD3を用いて暗号化されている。

【0111】ヘッダデータは、図7に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データKESC、sによる署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルIDに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ101の秘密鍵データKESC、sによる署名データが含まれる。なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図8に示すような情報を含めてもよい。また、コンテンツIDには、例えば、図9に示す情報が含まれている。コンテンツIDは、EMDサービスセンタ102あるいはコンテンツプロバイダ101において作成され、EMDサービスセンタ102において作成された場合には図9に示すようにEMDサービスセンタ102の秘密鍵データKESC、sによる署名データが添付され、コンテンツプロバイダ101において作成された場合にはコンテンツプロバイダ101の秘密鍵データKCP、sが添付される。コンテンツIDは、例えば、図4に示すように、コンテンツID生成部850が作成し、記憶部119に格納される。なお、コンテンツIDは、EMDサービスセンタ102が作成してもよい。

【0112】ディレクトリ構造データは、セキュアコンテンツ104内におけるコンテンツファイルCF相互間の対応関係と、コンテンツファイルCFとキーファイルFとの対応関係を示している。例えば、セキュアコンテ

ナ104内にコンテンツファイルCF₁～CF₃と、それらに対応するキーファイルKF₁～KF₃が格納されている場合には、図10に示すように、コンテンツファイルCF₁～CF₃相互間のリンクと、コンテンツファイルCF₁～CF₃とキーファイルKF₁～KF₃との間のリンク関係とがディレクトリ構造データによって確立される。ハイパーリンクデータは、セキュアコンテンツ104の内外の全てのファイルを対象として、キーファイルKF相互間の階層構造と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。具体的には、図11に示すように、セキュアコンテンツ104内にコンテンツファイルCFおよびキーファイルKF毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数H(x)を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【0113】また、権利書データ106には、図7に示すように、コンテンツID、コンテンツプロバイダ101の識別子CP_ID、権利書データ106の有効期限、EMDサービスセンタ102の通信アドレス、利用空間調査情報、販売価格情報、取扱方針、取扱制情報、商品デモ（試験）の取扱制情報およびそれらについての署名データなどが含まれる。なお、後述する第2実施形態のように、サービスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテンツ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテンツ104を提供するサービスプロバイダ310の識別子SP_IDが含まれる。

【0114】また、SAMプログラム・ダウンロード・コンテンツSDC₁～SDC₃には、図7に示すように、SAM105₁～105₄内でプログラムのダウンロードを行う際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ（UCP）U106のシンタックス（文法）を示すUCP-L（Label）、R（Reader）などのラベルリダと、SAM105₁～105₄に内蔵された記憶部（フラッシュROM）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。

【0115】なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベースを含む種々のデータベースを備えている。

【0116】署名処理部117は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ101の秘密鍵データKcp、sを用いて、その署名データSIGを作成する。

【0117】なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータ

に圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0118】セキュアコンテンツ作成部118は、図5（A）に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたメタデータMeta、コンテンツデータC、A/V仲長用ソフトウェアSoftwareおよび電子透かし情報モジュール（Watermark Module）WMとを格納したコンテンツファイルCFを生成する。

【0119】コンテンツファイルCFには、図6に示すように、ファイルリダと、秘密鍵データKcp、sによるファイルリダの署名データとを含むようにしてもよい。このようにすることで、SAM105₁～105₄において、異系列の複数のセキュアコンテンツ104から受信したそれぞれ異なるフォーマットのコンテンツファイルCFを格納した複数のセキュアコンテンツ104を効率的に処理できる。

【0120】ここで、ファイルリダは、コンテンツファイルCFおよびそれらに対応するキーファイルKFを流す際に用いられ、これらのファイルの読み込み手順などを示している。但し、本実施形態では、EMDサービスセンタ102からSAM105₁～105₄に、当該ファイルリダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテンツ104のコンテンツファイルCFは、ファイルリダを格納していない。

【0121】ヘッダデータには、図6に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データKcp、sによる署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルCFの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関する情報、およびディレクトリ情報などに関するコンテンツプロバイダ101の秘密鍵データKcp、sによる署名データが含まれる。

【0122】メタデータMetaには、図6に示すように、商品（コンテンツデータC）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。本発明では、図5および図6に示すように、コンテンツファイルCF内にメタデータMetaを格納して送信する場合を例示するが、メタデータMetaをコンテンツファイルCF内に格納せずに、コンテンツファイルCFを送信する経路とは別の経路でコンテンツプロバイダ101からSAM105₁などに送信してもよい。

【0123】A/V伸長用ソフトウェアSofitは、ユーザホームネットワーク103のネットワーク機器1601およびAV機器1602～1604において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、AT-RAC3方式の伸長用ソフトウェアである。このように、セキュアコンテナ104内にA/V伸長用ソフトウェアSofitを格納することで、SAM1051～1054においてセキュアコンテナ104内に格納されたA/V伸長用ソフトウェアSofitを用いてコンテンツデータCの伸長を行うことができ、コンテンツデータC何れかはコンテンツプロバイダ101毎にコンテンツデータCの圧縮および伸長方式をコンテンツプロバイダ101が自由に設定しても、ユーザに多大な負担をかけることはない。

【0124】電子透かし情報モジュールWMは、前述したように、例えば、コンテンツデータCに埋め込まれた電子透かし情報を検出するのに必要な情報およびソフトウェアを含んでいる。

【0125】また、セキュアコンテナ作成部118は、上述した図5(A)に示すコンテンツファイルCFと、当該コンテンツファイルCFの署名データSIGscpと、キーファイルデータベース118bから読み出した当該コンテンツファイルCFに対応する図5(B)に示すキーファイルKfと、当該キーファイルKfの署名データSIGkcpと、記憶部119から読み出したコンテンツプロバイダ101の公開鍵証明書データCERcpと、当該公開鍵証明書データCERcpの署名データSIG1、ESCとを格納したセキュアコンテナ104を生成する。

【0126】ここで、署名データSIGscpは、セキュアコンテナ104の受信先において、コンテンツファイルCFの作成者および送信者の正当性を検証するために用いられる。ここで、署名データSIGkcpは、セキュアコンテナ104の受信先において、キーファイルKfの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ104の受信先において、キーファイルKfの作成者の正当性の検証は、キーファイルKf内の署名データSIGk1、ESCに基づいて行われる。また、署名データSIGk1、ESCは、キーファイルKfが、EMDサービスセンタ102に登録されているか否かを検証するためにも用いられる。

【0127】本実施形態では、コンテンツデータCの圧縮方式、圧縮の有無、暗号化方式（共通暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータCを得た信号の語元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータCがセキュアコンテナ104内に格納されている。すなわち、これらの事項をコンテンツプロバイダ101が自由に決

定できる。

【0128】また、セキュアコンテナ作成部118は、セキュアコンテナデータベース118aに格納したセキュアコンテナ104を、ユーザからの要求に応じてSAM管理部124に出力する。このように、本実施形態では、コンテンツプロバイダ101の公開鍵データCERcpの公開鍵証明書CERcpをセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド（In-band）方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CERcpを得るための通信をEMDサービスセンタ102との間で行う必要がない。なお、本発明では、公開鍵証明書CERcpをセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書CERcpを得るアウト・オブ・バンド（Out-of-band）方式を採用してもよい。

【0129】相互認証部120は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ（共有鍵）Ksesを生成する。セッション鍵データKsesは、相互認証を行う度に新たに生成される。

【0130】暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データKsesを用いて暗号化する。また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データKsesを用いて復号する。

【0131】権利書データ作成部122は、権利書データ106を作成し、これをEMDサービスセンタ管理部125に出力する。権利書データ106は、コンテンツデータCの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP（Suggested Retailer's Price）やコンテンツデータCの複製ルールなどが記述されている。

【0132】SAM管理部124は、セキュアコンテナ104を、オフラインおよび/またはオンラインでユーザホームネットワーク103に供給する。また、SAM管理部124は、セキュアコンテナ104をオンラインでSAM1051～1054に配給する場合には、セキュアコンテナ104を送信する通信プロトコルとして、デジタル放送であればMHG（Multimedia and Hypermedia information

n coding Experts Group) プロトコルを用い、インターネットであればXML/SMIL/HTML (Hyper Text Markup Language) を用い、これらの通信プロトコル内に、セキュアコンテンツ104を、符号化方式に依存しない形式でトンネリングして埋め込む。従って、通信プロトコルとセキュアコンテンツ104との間でフォーマットの整合性をとる必要性はなく、セキュアコンテンツ104のフォーマットを柔軟に設定できる。なお、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテンツ104を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。

【0133】図12は、本実施形態で用いられるROM型の記録媒体1301を説明するための図である。図12に示すように、ROM型の記録媒体1301は、ROM領域131、セキュアRAM領域132およびメディアSAM133を有する。ROM領域131には、図5(A)に示したコンテンツファイルCFが記憶されている。また、セキュアRAM領域132は、記憶データに対してのアクセスに所定の許可(認証)が必要な領域であり、図5(B)、(C)に示したキーファイルKFおよび公開鍵証明書データCERTおよび機種の種類に応じて固有の値を持つ記録用鍵データKSKとを収容してMAC(Message Authentication Code)関数を用いて生成した署名データと、当該キーファイルKFおよび公開鍵証明書データCERTとを記録媒体に固有の値を持つメディア鍵データKMDNを用いて暗号化したデータとが記憶される。また、セキュアRAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM1051~1055を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。また、セキュアRAM領域132には、後述するようにユーザホームネットワーク103のSAM1051~1055においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御状態データ166がセキュアRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体1301となる。メディアSAM133には、例えば、ROM型の記録媒体1301の識別子であるメディアIDと、メディア鍵データKMDNとが記憶されている。メディアSAM133は、例えば、相互認証機能を有している。

【0134】本実施形態で用いるROM型の記録媒体としては、例えば、図12に示すもの他に、図13に示すROM型の記録媒体1302および図14に示すROM型の記録媒体1303なども考えられる。図13に示すROM型の記録媒体1302は、ROM領域131と認証機能を有するメディアSAM133とを有し、図1

2に示すROM型の記録媒体1301のようにセキュアRAM領域132を備えていない。ROM型の記録媒体1302を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図14に示すROM型の記録媒体1303は、ROM領域131およびセキュアRAM領域132を有し、図12に示すROM型の記録媒体1301のようにメディアSAM133を有していない。ROM型の記録媒体1303を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記憶する。また、ROM型の記録媒体1303を用いる場合には、SAMとの間で相互認証は行わない。また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いられる。

【0135】本実施形態で用いるRAM型の記録媒体としては、例えば図15に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRAM領域134を有するRAM型の記録媒体1304がある。RAM型の記録媒体1304では、メディアSAM133は認証機能を持ち、キーファイルKFを記憶する。また、RAM領域134には、コンテンツファイルCFが記録される。また、本実施形態で用いるRAM型の記録媒体としては、その他に、図16に示すRAM型の記録媒体1350および図17に示すRAM型の記録媒体1306なども考えられる。図16に示すRAM型の記録媒体1306は、セキュアでないRAM領域134と認証機能を有するメディアSAM133とを有し、図15に示すRAM型の記録媒体1304のようにセキュアRAM領域132を備えていない。RAM型の記録媒体1306を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図17に示すRAM型の記録媒体1306は、セキュアRAM領域132およびセキュアでないRAM領域134を有し、図15に示すRAM型の記録媒体1304のようにメディアSAM133を有していない。RAM型の記録媒体1306を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記憶する。また、RAM型の記録媒体1306を用いる場合には、SAMとの間で相互認証は行わない。

【0136】また、SAM管理部124は、セキュアコンテンツ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データKSKSを用いてセキュアコンテンツ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。本実施形態では、SAM管理部、EMDサービスセンサ管理部、並びに後述す

77

るコンテンツプロバイダ管理部およびサーバプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0137】ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテンツ104を用いる。従って、ユーザホームネットワーク103のSAM1051~1054では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0138】また、上述したように、本実施形態では、セキュアコンテンツ104内に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データKcとを同時するイン・バンド（In-Band）方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データKcを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データKcは配信用鍵データKDi~KD6で暗号化されているが、配信用鍵データKDi~KD6は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM1051~1054に事前に（SAM1051~1054がEMDサービスセンタ102に初回にアクセスする際に）配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。なお、本発明は、後述するようにコンテンツデータCとコンテンツ鍵データKcとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド（Out-Of-Band）方式を採用できる柔軟性を有している。

【0139】EMDサービスセンタ管理部125は、EMDサービスセンタ102から決済レポートデータ107を受信すると、これを暗号化・復号部121においてセッション鍵データKsesを用いて復号した後に、記憶部119に記憶する。決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行ったコンテンツプロバイダ101に関する決済の内容が記述されている。

【0140】また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク（Global Unique）な識別子であるコンテンツID、公開鍵データKcp、pおよびそれらの署名データSIGcpを、EMDサービスセンタ102

78

に送信し、EMDサービスセンタ102から、公開鍵データKcp、pの公開鍵証明書データCERcpを入力する。また、EMDサービスセンタ管理部125は、コンテンツデータCのそれぞについて、コンテンツ鍵データKc、権利書データ106および電子透かし情報管理データWMをEMDサービスセンタ102に登録してキーファイルKFを受ける際に、図18に示すように、提供するコンテンツデータCのグローバルユニークな識別子であるコンテンツID、コンテンツ鍵データKc、権利書データ106、電子透かし情報管理データWM、コンテンツプロバイダ101のグローバルユニークな識別子であるCP_IDと、それらについてのコンテンツプロバイダ101の秘密鍵データKcp、sによる署名データSIGcp、sとを格納した登録モジュールModxを作成する。そして、EMDサービスセンタ管理部125は、登録モジュールModxを暗号化・復号部121においてセッション鍵データKsesを用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0141】以下、図3および図4を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶されている。

【0142】まず、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データKcp、sに対応する公開鍵データKcp、sの正当性を証明する公開鍵証明書データCERcpを要求する場合の処理を図4を参照しながら説明する。コンテンツプロバイダ101は、真性乱数発生器を用いて乱数を発生して秘密鍵データKcp、sを生成し、当該秘密鍵データKcp、sに対応する公開鍵データKcp、pを作成して記憶部119に記憶する。EMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子CP_IDおよび公開鍵データKcp、pを記憶部119から読み出す。そして、EMDサービスセンタ管理部125は、当該登録に応じた公開鍵証明書データCERcpおよびその署名データSIGcp、escをEMDサービスセンタ102から入力して記憶部119に書き込む。

【0143】次に、コンテンツプロバイダ101が、EMDサービスセンタ102にコンテンツ鍵データKc、権利書データ106および電子透かし情報管理データWMを登録し、コンテンツデータCに対応するキーファイルKFを受信する場合の処理を図4、図18および図19を参照して説明する。権利書データ106などの登録は、個々のコンテンツデータCについてそれぞれ行われる。図19は、コンテンツプロバイダ101からEMDサービスセンタ102への登録処理を説明するためのフローチャートである。

【0144】ステップA1：図4に示すコンテンツプロバイダ101の相互認証部120とEMDサービスセンタ102との間で相互認証を行う。

ステップA2：ステップA1で行った相互認証によって得られたセッション鍵データKsesをコンテンツプロバイダ101およびEMDサービスセンタ102で共有する。

【0145】ステップA3：コンテンツプロバイダ101は、記憶部119などのデータベースから、EMDサービスセンタ102に登録を行うコンテンツID、コンテンツ鍵データKc、権利書データ106、電子透かし情報管理データWMおよびCPIDなどを読み出す。

ステップA4：署名処理部117において、コンテンツプロバイダ101の秘密鍵データKcp_sを用いて、ステップA3で読み出した権利書データ106などを含むモジュールに対して、送り主の正当性を示す署名データSIGm1_cpを作成する。そして、EMDサービスセンタ管理部125は、図18に示すように、コンテンツID、コンテンツ鍵データKc、権利書データ106、電子透かし情報管理データWMおよびCPIDと、これらについての署名データSIGm1_cpとを格納した登録用モジュールMod2を作成する。

【0146】ステップA5：暗号化・復号部121は、ステップA4で作成した登録用モジュールMod2を、ステップA2で共有したセッション鍵データKsesを用いて暗号化する。

ステップA6：EMDサービスセンタ管理部125は、ステップA5で暗号化した登録用モジュールMod2をEMDサービスセンタ102に送信する。

【0147】ステップA7以降の処理は、EMDサービスセンタ102における処理である。

ステップA7：EMDサービスセンタ102は、受信した登録用モジュールMod2を、ステップA2において共有したセッション鍵データKsesを用いて復号する。

ステップA8：EMDサービスセンタ102は、復号した登録用モジュールMod2に格納された署名データSIGm1_cpを公開鍵データKcp_pを用いて検証し、登録用モジュールMod2の送り主の正当性を確認し、送り主の正当性が証明されたことを条件にステップ

A9の処理を行う。

ステップA9：EMDサービスセンタ102は、登録用モジュールMod2に格納されているコンテンツID、コンテンツ鍵データKc、権利書データ106、電子透かし情報管理データWMおよびCPIDを所定のデータベースに格納して登録する。

【0148】なお、EMDサービスセンタ管理部125は、図18に示すように、登録用モジュールMod2に応じた登録処理がEMDサービスセンタ102に行われた後に、例えば6カ月分のキーファイルKFをEMDサービスセンタ102から受信し、相互認証部120とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データKsesを用いて、当該受信したキーファイルKFを復号した後にキーファイルデータベース118bに記憶する。

【0149】次に、コンテンツプロバイダ101がユーザホームネットワーク103のSAM1051にセキュアコンテナ104を送信する場合の処理を図3および図4を参照しながら説明する。なお、以下の例では、コンテンツプロバイダ101からSAM1051にセキュアコンテナ104を送信する場合を示すが、セキュアコンテナ104をSAM1052～1054に送信する場合も、SAM1051を介してSAM1052～1054に送信される点を除いて同じである。先ず、図3に示すように、コンテンツデータS111がコンテンツマスターデータベース111から読み出されて電子透かし情報付加部112に出力される。次に、電子透かし情報付加部112は、コンテンツデータS111に電子透かし情報を埋め込んでコンテンツデータS112を生成し、これを圧縮部113に出力する。次に、圧縮部113は、コンテンツデータS112を、例えばATRAC3方式で圧縮してコンテンツデータS113を作成し、これを暗号化部114に出力する。また、図4に示すように、乱数発生部115において、乱数を生じさせてコンテンツ鍵データKcが生成され、当該生成されたコンテンツ鍵データKcが記憶部119に記憶される。

【0150】次に、暗号化部114は、圧縮部113から入力したコンテンツデータS113と、記憶部119から読み出したメタデータMeta、A/V伸長用ソフトウェアSoftおよび電子透かし情報管理データWMとを、コンテンツ鍵データKcを用いて暗号化してセキュアコンテナ作成部118に出力する。この場合に、メタデータMetaおよび電子透かし情報管理データWMは暗号化しなくてもよい。そして、セキュアコンテナ作成部118は、図5(A)に示すコンテンツファイルCFを作成する。また、署名処理部117において、コンテンツファイルCFのハッシュ値がとられ、秘密鍵データKcp_sを用いて署名データSIGm1_cpが生成される。

【0151】また、セキュアコンテナ作成部118は、

キープファイルデータベース118bから、コンテンツデータCに対応するキープファイルKFを読み出し、これを署名処理部117に出力する。そして、署名処理部117は、セキュアコンテナ作成部118から入力したキープファイルKFのハッシュ値と、秘密鍵データKcpr、sを用いて署名データSIGr、cpを生成し、これをセキュアコンテナ作成部118に出力する。次に、セキュアコンテナ作成部118は、図5(A)に示すコンテンツファイルCFおよびその署名データSIGr、cpと、図5(B)に示すキープファイルKFおよびその署名データSIGr、cpと、記憶部119から読み出した図5(C)に示す公開鍵証明書データCERcpおよびその署名データSIGr、escとを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。そして、セキュアコンテナ作成部118は、例えばユーザからの要求(リクエスト)に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118aから読み出して、相互認証部120とSAM105との間の相互認証によって得られたセッション鍵データKsesを用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM105に送信する。

【0152】以下、コンテンツプロバイダ101の処理の全体の流れの概要を、セキュアコンテナ作成処理と関連付けて述べる。図20、図21、図22は、当該処理の流れを説明するためのフローチャートである。

ステップB1: コンテンツプロバイダ101は、予め自らの公開鍵証明書データCERcpをEMDサービスセンタ102から入力し、記憶部(データベース)119に格納しておく。

ステップB2: 新しいオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツIDを割り振る、コンテンツマスタソースデータベース111に格納して一元的に管理する。

ステップB3: ステップB1において一元的に管理した各々のコンテンツマスタソースにメタデータMetaを作成し、これを記憶部119に格納する。

【0153】ステップB4: コンテンツマスタソースデータベース111からコンテンツマスタソースであるコンテンツデータS111を読み出して電子透かし情報付加部112に出力し、電子透かし情報を埋め込んでコンテンツデータS112を生成する。

ステップB5: 電子透かし情報付加部112は、埋め込みを行った電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップB6: 圧縮部113において、電子透かし情報が埋め込まれたコンテンツデータS112を圧縮してコ

ンテンツデータS113を生成する。

ステップB7: 伸長部116において、圧縮されたコンテンツデータS113を伸長してコンテンツデータS116を生成する。

ステップB8: 悪意検査部123において、伸長したコンテンツデータS116の悪意検査を行う。

ステップB9: コンテンツプロバイダ101は、コンテンツデータS116に埋め込まれた電子透かし情報を、ステップB5でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。そして、コンテンツプロバイダ101は、悪意検査および電子透かし情報の検出の双方が成功した場合には、ステップB10の処理を行い、何れか一方が失敗した場合にはステップB4の処理を繰り返す。

【0154】ステップB10: 乱数発生部115において乱数としてコンテンツ鍵データKcを生成し、これを記憶部119に格納する。

ステップB11: 暗号化部114において、圧縮したコンテンツデータS113を、コンテンツ鍵データKcを用いて暗号化してコンテンツデータCを作成する。

【0155】ステップB12: 権利書データ作成部122において、コンテンツデータCについての権利書データ106を作成する。

ステップB13: コンテンツプロバイダ101は、SRPを決定し、これを記憶部119に格納する。

ステップB14: コンテンツプロバイダ101は、コンテンツID、コンテンツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力する。

ステップB15: コンテンツプロバイダ101は、配信用鍵データKD1~KD8で暗号化されたキープファイルKFをEMDサービスセンタ102から入力する。

ステップB16: コンテンツプロバイダ101は、入力したキープファイルKFをキープファイルデータベース118bに格納する。

【0156】ステップB17: コンテンツプロバイダ101は、コンテンツデータCとキープファイルKFとのリンク関係をハイパーリンクで結ぶ。

ステップB18: 署名処理部117において、コンテンツデータCおよびキープファイルKFの各々について、秘密鍵データKcp、sを用いて、作成者の正当性を署名データを作成する。

ステップB19: セキュアコンテナ作成部118において、図5に示すセキュアコンテナ104を作成する。

【0157】ステップB20: 複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップB1~B19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキープファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク関係とをハイパーリンクなどを用いて結ぶ。

ステップB21:コンテンツプロバイダ101は、作成したセキュアコンテナ104をセキュアコンテナデータベース118aに格納する。

【0158】[EMDサービスセンタ102] EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing)(利益分配)機能を有する。

図23は、EMDサービスセンタ102の機能の構成図である。図23に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利管理管理部145、権利書データベース145a、証明書データベース145b、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151およびKF作成部153を有する。なお、図23には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流が示されている。また、図24には、EMDサービスセンタ102内の機能ブロック相互間のデータの流のうちの、SAM105:~105aおよび図1に示す決済機関91との間で送受信されるデータに関連するデータの流が示されている。

【0159】鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて6か月分組み出してSAM管理部149に出力する。また、鍵データベース141a配信用鍵データKDの他に、EMDサービスセンタ102の秘密鍵データKESC、登録用鍵データKSTR、メディア鍵データKMEDおよびMAC鍵データKMACなどの鍵データを記憶する一連の鍵データを格納している。

【0160】決算処理部142は、SAM105:~105aから入力した利用履歴データ108と、証明書・権利管理管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144に出力する。なお、決算処理部142は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。ここで、利用履歴データ108は、ユーザホームネットワーク103におけるセキュアコンテナ104の購入、利用(再生、記録および転送など)の履歴を示し、決算処理部142においてセキュアコンテナ104に関連したライセンス料の支払い額を決定する際に用いられる。

【0161】利用履歴データ108には、例えば、セキ

ュアコンテナ104に格納されたコンテンツデータCの識別子であるコンテンツID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105:~105aの識別子SAM_ID、当該SAM105:~105aのユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

【0162】また、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。なお、決済機関91は、決済が終了すると、当該決済機関の利用明細書をEMDサービスセンタ102に送る。EMDサービスセンタ102は、当該利用明細書の内容を、対応する権利者に通知する。

【0163】決算機関管理部144は、決算処理部142が生成した決済請求権データ152を図1に示すバイメントゲートウェイ90を介して決済機関91に送信する。なお、後述するように、決算機関管理部144は、決済請求権データ152を、コンテンツプロバイダ101などの権利者に送信し、受信した決済請求権データ152を用いて、権利者自らが決済機関91に対しての決済を行ってもよい。また、決算機関管理部144は、署名処理部143において決済請求権データ152のハッシュ値をとり、秘密鍵データKESCを用いて生成した署名データSIGaを決済請求権データ152と共に決済機関91に送信する。

【0164】証明書・権利管理管理部145は、証明書データPES145bに登録(記録)されて権威化された公開鍵証明書データCERCPおよび公開鍵証明書データCERSAM1~CERSAM4などを読み出すと共に、コンテンツプロバイダ101の権利書データ106、コンテンツ鍵データKcおよび電子透かし情報管理データWMなどを権利書データベース145aに登録して権威化する。ここで、権利書データベース145aはコンテンツIDを検索キーとして検索が行われ、証明書データベース145bはコンテンツプロバイダ101の識別子CP_IDを検索キーとして検索が行われる。また、証明書・権利管理管理部145は、例えば、権利書デ

85

ータ106、コンテンツ鍵データKcおよび電子透かし情報管理データWMなどのハッシュ値をとり、秘密鍵データK_{ESC}を用いた署名データを付した極密化されたデータを権利書データベース145aに格納する。

【0165】コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されたコンテンツプロバイダ101の識別子C P_IDなどを管理するCPデータベース148aにアクセスできる。

【0166】SAM管理部149は、ユーザホームネットワーク103内のSAM1051~1054との間で通信する機能を有し、登録されたSAMの識別子SAM_IDやSAM登録リストなどを記録したSAMデータベース149aにアクセスできる。

【0167】KF作成部153は、コンテンツプロバイダ管理部148から入力したコンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC1~SDCnとを署名処理部143に出力する。また、KF作成部153は、鍵サーバ141から入力した対応する期間の配信用鍵データKD1~KDnを用いて、コンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1~SDCnを暗号化し、図5(B)に示すように、当該暗号化したデータと、署名処理部143から入力した当該暗号化したデータについての秘密鍵データK_{ESC}による署名データSIG_{K1,ESC}とを格納したキヤファイルKFを作成し、当該作成したキヤファイルKFをKFデータベース153aに格納する。

【0168】以下、EMDサービスセンタ102内での処理の流れを説明する。まず、EMDサービスセンタ102からユーザホームネットワーク103内のSAM1051~1054に配信用鍵データを送信する際の処理の流れを、図24を参照しながら説明する。図24に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データKD1~KDnを鍵データベース141aから読み出してSAM管理部149に出力する。また、署名処理部143は、配信用鍵データKD1~KDnの各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC}を用いて、それぞれに対応する署名データSIG_{KD1,ESC}~SIG_{KDn,ESC}を作成し、これをSAM管理部149に出力する。SAM管理部149は、この3カ月分の配信用鍵データKD1~KDnおよびそれらの署名データSIG_{KD1,ESC}~SIG_{KDn,ESC}を、相互認証部150とSAM1051~1054と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM1051~1054に送信する。

【0169】次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データCER

86

RcPの発行要求を受けた場合の処理を、図23を参照しながら説明する。この場合に、コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子C P_ID、公開鍵データKcP、および署名データSIG_{CP,CP}をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データSIG_{CP,CP}の正当性を署名処理部143

10において確認した後に、識別子C P_IDおよび公開鍵データKcP、Pに基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。そして、証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データCER_{CP}を証明書データベース145bから読み出してコンテンツプロバイダ管理部148に出力する。また、署名処理部143は、公開鍵証明書データCER_{CP}のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC}を用いて、署名データSIG_{1,ESC}を作成し、これをコンテンツプロバイダ管理部148に出力する。そして、コンテンツプロバイダ管理部148は、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}を、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0170】次に、EMDサービスセンタ102がSAM1051から、公開鍵証明書データCER_{SAM1}の発行要求を受けた場合の処理を、図24を参照しながら説明する。この場合に、SAM管理部149は、SAM1051の識別子SAM1_ID、公開鍵データK_{SAM1}、および署名データSIG_{SAM1}をSAM1051から受信すると、これらを、相互認証部150とSAM1051と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データSIG_{SAM1}の正当性を署名処理部143において確認した後に、識別子SAM1_IDおよび公開鍵データK_{SAM1}、Pに基づいて、当該公開鍵証明書データの発行要求を出したSAM1051がSAMデータベース149aに登録されているか否かを確認する。そして、証明書・権利書管理部145は、当該SAM1051の公開鍵証明書データCER_{SAM1}を証明書データベース145bから読み出してSAM管理部149に出力する。また、署名処理部143は、公開鍵証明書データCER_{SAM1}のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC}を用いて、署名データSIG_{SAM1,ESC}を作成し、これをSAM管理部149に出力する。そして、SAM管理部149は、公開鍵証明書データCER

SAM1およびその署名データSIG500、ESCを、相互認証部150とSAM1051との間の相互認証で得られたセッション鍵データKSESを用いて暗号化した後に、SAM1051に送信する。なお、SAM1052～1054が、公開鍵証明書データを要求した場合の処理は、対象がSAM1052～1054に代わるのみで、基本的に上述したSAM1051の場合と同じである。なお、本発明では、EMDサービスセンタ102は、例えば、SAM1051の出荷時に、SAM1051の秘密鍵データK_{SAM1}、sおよび公開鍵データK_{SAM1}、PをSAM1051の記憶部に記憶する場合には、当該出荷時に、公開鍵データK_{SAM1}、Pの公開鍵証明書データCER_{SAM1}を作成してもよい。このとき、当該出荷時に、公開鍵証明書データCER_{SAM1}を、SAM1051の記憶部に記憶してもよい。

【0171】次に、EMDサービスセンタ102が、コンテンツプロバイダ101から図18に示す登録用モジュールMod2を受けた場合の処理を、図23を参照しながら説明する。この場合には、コンテンツプロバイダ管理部148がコンテンツプロバイダ101から図18に示す登録用モジュールMod2を受信すると、相互認証部150と図4に示す相互認証部120との間の相互認証で得られたセッション鍵データKSESを用いて登録用モジュールMod2を復号する。そして、署名処理部143において、鍵データベース141aから読み出した公開鍵データK_{EP}、Pを用いて、署名データSIG_{M1}、CPの正当性を検証する。次に、証明書・権利書管理部145は、登録用モジュールMod2に格納された権利書データ106、コンテンツ鍵データKc、電子透かし情報管理データWMおよびSRPを、権利書データベース145aに登録する。

【0172】次に、コンテンツプロバイダ管理部148は、コンテンツ鍵データKcおよび権利書データ106をKF作成部153に出力する。次に、KF作成部153は、コンテンツプロバイダ管理部148から入力したコンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC1～SDC4とを署名処理部143に出力する。そして、署名処理部143は、KF作成部153から入力したデータ全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC}、sを用いて、その署名データSIG_{K1}、ESCを作成し、これをKF作成部153に出力する。次に、KF作成部153において、鍵サーバ141から入力した対応する期間の配信用鍵データKD1～KD4を用いて、コンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC1～SDC4を暗号化し、当該暗号化したデータと、署名処理部143から入力した署名データSIG_{K1}、ESCとを格納したキー

ファイルKFを作成し、これをKFデータベース153aに格納する。ここで、SAMプログラム・ダウンロード・コンテナSDC1～SDC4は、登録用モジュールMod2内に格納したものをを用いても、あるいはEMDサービスセンタ102が予め保持しているものを用いてもよい。次に、コンテンツプロバイダ管理部148は、KFデータベース153aにアクセスを行って得たキーファイルKFを、相互認証部150と図4に示す相互認証部120との間の相互認証で得られたセッション鍵データKSESを用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0173】次に、EMDサービスセンタ102において行なう決済処理を図24を参照しながら説明する。SAM管理部149は、ユーザホームネットワーク103の例えばSAM1051から利用履歴データ108およびその署名データSIG200、SAM1を入力すると、利用履歴データ108および署名データSIG200、SAM1を、相互認証部150とSAM1051との間の相互認証によって得られたセッション鍵データKSESを用いて復号し、SAM1051の公開鍵データK_{SAM1}による署名データSIG200、SAM1の検証を行なった後に、決済処理部142に出力する。

【0174】そして、決済処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書・権利書管理部145を介して権利書データベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。決済処理部142は、決済請求権データ152を決済機関管理部144に出力すると共に、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

【0175】次に、決済機関管理部144は、決済請求権データ152およびその署名データSIG200を、相互認証およびセッション鍵データKSESによる復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

【0176】次に、EMDサービスセンタ102がコンテンツプロバイダ101に決済レポートを送信する場合の処理を図23を参照しながら説明する。決済処理部142において決済が行なわれると、前述したように、決済処理部142からコンテンツプロバイダ管理部148に決済レポートデータ107が出力される。決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。EMDサービスセンタ102は、決済処理部142から決済レポートデータ107を入力

すると、これを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0177】また、EMDサービスセンタ102は、前述したように、権利書データ106を登録（権威化）した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、権威化証明書モジュールを配信用鍵データKD₁～KD_nで暗号化して送信してもよい。

【0178】また、EMDサービスセンタ102は、その他に、SAM105₁～105_nの出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

【0179】【ユーザホームネットワーク103】ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160₁およびA/V機器160₂～160_nを有している。ネットワーク機器160₁は、SAM105₁を内蔵している。また、A/V機器160₂～160_nは、それぞれSAM105₂～105_nを内蔵している。SAM105₁～105_nの相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。なお、A/V機器160₂～160_nは、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160₁のネットワーク通信機能を利用していてもよい。また、ユーザホームネットワーク103は、ネットワーク機能を有していないA/V機器のみを有していてもよい。

【0180】以下、ネットワーク機器160₁について説明する。図25は、ネットワーク機器160₁の構成図である。図25に示すように、ネットワーク機器160₁は、SAM105₁、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

【0181】SAM105₁～105_nは、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。SAM105₁～105_nは、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁～105_nのIC(Integrated Circuit)の内部の仕様を知ることではできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それによってネットワーク機器160₁およびA/V機器160₂～160_nに搭載される。

【0182】SAM105₁～105_nは、その処理内

容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)である。SAM105₁～105_nの機能はICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【0183】以下、SAM105₁の機能について詳細に説明する。なお、SAM105₂～105_nは、SAM105₁と基本的に同じ機能を有している。図26は、SAM105₁の機能の構成図である。なお、図26には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。図26に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック(作業)メモリ200および外部メモリ管理部811を有する。なお、A/V機器160₂～160_nはダウンロードメモリ167を有していないため、SAM105₂～105_nにはダウンロードメモリ管理部182は存在しない。

【0184】なお、図26に示すSAM105₁の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。また、外部メモリ201には、以下に示す処理を経て、図27に示すように、利用履歴データ108およびSAM登録リストが記憶される。ここで、外部メモリ201のメモリ空間は、SAM105₁の外部(例えば、ホストCPU810)からは見ることができず、SAM105₁のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。外部メモリ201としては、例えば、フラッシュメモリあるいは揮発性メモリ(FE RAM)などが用いられる。また、スタックメモリ200としては、例えばSARAMが用いられ、図28に示すように、セキュアコンテナ104、コンテンツ鍵データK_c、権利書データ(UCP)106、記憶部192のロック鍵データK_{LOC}、コンテンツプロバイダ101の公開鍵証明書CER_{CP}、利用履歴状態データ(UCS)186、およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC_nなどが記憶される。

【0185】以下、SAM1051の機能のうち、コンテンツプロバイダ101からのセキュアコンテンツ104を入出力したときの各機能ブロックの処理内容を図26を参照しながら説明する。

【0186】相互認証部170は、SAM1051がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ(共有鍵)Ksesを生成し、これを暗号化・復号部171に出力する。セッション鍵データKsesは、相互認証を行う度に新たに生成される。

【0187】暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データKsesを用いて暗号化・復号する。

【0188】誤り訂正部181は、セキュアコンテンツ104を読み訂正してダウンロードメモリ管理部182に出力する。なお、ユーザホームネットワーク103は、セキュアコンテンツ104が改竄されているか否かを検出する機能を持ててもよい。本実施形態では、誤り訂正部181を、SAM1051に内蔵した場合を示したが、誤り訂正部181の機能を、例えばホストCPU810などのSAM1051の外部に持たせてもよい。

【0189】ダウンロードメモリ管理部182は、図25に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテンツ104を、相互認証によって得られたセッション鍵データKsesを用いて暗号化して図25に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図29に示すように、HDD(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図26に示すスタックメモリ200にダウンロードする。

【0190】セキュアコンテンツ復号部183は、ダウンロードメモリ管理部182から入力したセキュアコンテンツ104に格納されたキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテンツSDC1~SDCnを、記憶部192から読み出した対応する期間の配信用鍵データKD1~KDnを用いて復号する。当該復号されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテンツSDC1~S

DCnは、スタックメモリ200に書き込まれる。

【0191】EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0192】署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データKesc、rおよびコンテンツプロバイダ101の公開鍵データKcp、rを用いて、セキュアコンテンツ104内の署名データの検証を行う。

【0193】記憶部192は、SAM1051の外部から読み出しおよび書き換えできない秘密データとして、図30に示すように、有効期限付きの複数の配信用鍵データKD1~KDn、SAM_ID、ユーザID、パスワード、情報参照用ID、SAM登録リスト、記録用鍵データKstr、ルートCAの公開鍵データKrc、A、P、EMDサービスセンタ102の公開鍵データKesc、r、メディア鍵データKmed、EMDサービスセンタ102の公開鍵データKesc、r、SAM1051の秘密鍵データKSAMI、s、SAM1051の公開鍵データKSAMI、rを格納した公開鍵証明書CERSAMI、EMDサービスセンタ102の秘密鍵データKesc、sを用いた公開鍵証明書CERescの署名データSIG22、復号・伸長モジュール163との間の相互認証用の元鍵データ(共通鍵暗号化方式を採用した場合)、メディアSAMとの間の相互認証用の元鍵データ(共通鍵暗号化方式を採用した場合)、並びにメディアSAMの公開鍵証明書格納用CERMEDSAM(公開鍵暗号化方式を採用した場合)を記憶している。また、記憶部192には、図26に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。記憶部192としては、例えば、フラッシュEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0194】以下、EMDサービスセンタ102から受信した配信用鍵データKD1~KDnを記憶部192に格納する際のSAM1051内での処理の流れを図26を参照しながら説明する。この場合には、まず、相互認証部170と図23に示す相互認証部150との間で相互認証が行われる。次に、当該相互認証によって得られたセッション鍵データKsesで暗号化された3カ月の配信用鍵データKD1~KDnおよびその署名データSIGKD1、esc~SIGKDn、escが、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。次に、暗号化・復号部171において、セッション鍵データKsesを用いて、配信用鍵データKD1~KDnおよびその署名データSIGKD1、esc~SIGKDn、escが復号される。次に、署名処理部189において、スタックメモリ811に記憶された署名デ

93

ークSIGKD1、ESC～SIGKD3、ESCの正当性が確認された後に、配信用鍵データKD1～KD3が記憶部192に書き込まれる。

【0195】以下、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM1051内での処理の流れを図26を参照しながら説明する。図26に示すSAM1051の相互認証部170と図3に示す相互認証部120との間で相互認証が行なわれる。暗号化・復号部171は、当該相互認証によって得られたセッション鍵データKSESを用いて、コンテンツプロバイダ管理部180を介してコンテンツプロバイダ101から供給されたセキュアコンテナ104を復号する。

【0196】次に、署名処理部189は、図5(C)に示す署名データSIG1、ESCの検証を行なった後に、図5(C)に示す公開鍵証明書データCERTCP内に格納されたコンテンツプロバイダ101の公開鍵データKCP、Pを用いて、署名データSIG6、CP、SIG7、CPの正当性を検証する。このとき、署名データSIG8、CPが正当であると検証されたときに、コンテンツファイルCFの作成者および送信者の正当性が確認される。また、署名データSIG7、CPが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。また、署名処理部189は、記憶部192から読み出した公開鍵データKRS、Pを用いて、図5(B)に示すキーファイルKF内の署名データSIGK1、ESCの正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。コンテンツプロバイダ管理部180は、署名データSIG6、CP、SIG7、CP、SIGK1、ESCの正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する。

【0197】誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104をダウンロードメモリ167に書き込む。

【0198】次に、ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図5(B)に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0199】そして、セキュアコンテナ復号部183において、記憶部192から入力した対応する期間の配信用鍵データKD1～KD3を用いて、図5(B)に示すキーファイルKF内のコンテンツ鍵データKC、権利書データ106およびSAMプログラム・ダウンロード・

94

コンテナSDC1～SDC3が復号される。そして、復号されたコンテンツ鍵データKC、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1～SDC3がスタックメモリ200に書き込まれる。

【0200】以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図31を参照しながら説明する。

【0201】利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ106は、図26を用いて説明したように、復号後にKFに格納されてスタックメモリ200に記憶されている。また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

【0202】課金処理部187は、図25に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0203】また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図5(B)に示すキーファイルKFの権利書データ106内に格納されている。課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0204】また、課金処理部187は、操作信号S165に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御状態(UCS: Usage Control Status)データ166を生成し、これをスタックメモリ200に書き込む。コンテンツの購入形態としては、例えば、購入による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該

決定された購入形態で評価された範囲内でユーザが当該コンテンツの利用を行うように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行われたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0205】なお、決定された購入形態が再生課金である場合には、例えば、SAM1051からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM1051に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0206】EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データKSAM1、を用いて利用履歴データ108の署名データSIG200、SAM1を作成し、署名データSIG200、SAM1を利用履歴データ108と共にEMDサービスセンタ102に送信する。EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0207】ダウンロードメモリ管理部182は、例えば、図25に示す購入形態決定操作部165からの操作信号S185に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。また、復号・伸長モジュール管理部184は、図25に示す購入形態決定操作部165からの操作信号S185に応じてコンテンツの試験動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

【0208】ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試験モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ(信号)を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試験時の再生機能を限定したり、試験可能な期間を限定するものなどがある。

【0209】以下、SAM1051内での処理の流れについて説明する。まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテンツ104の購入形態を決定するまでの処理の流れを図31を参照しながら説明する。ユーザによる図25に示す購入・利用形態決定操作部165の操作によって、試験モードを示す操作信号S165が課金処理部187に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図25に示す復号・伸長モジュール163に出力される。このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKsesによる暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データKsesによる暗号化・復号とが行われる。コンテンツファイルCFは、図25に示す復号部221においてセッション鍵データKsesを用いて復号された後に、復号部222に出力される。

【0210】また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図25に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データKsesによる暗号化および復号が行われる。次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

【0211】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。そして、課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。以後は、利用監視部186において、利用制

【0212】そして、後述する図34(C)に示す新たなキーファイルKF_iが作成され、当該作成されたキーファイルKF_iがダウンロードメモリ管理部182を介してダウンロードメモリ167に記憶される。図34(C)に示すように、キーファイルKF_iに格納された利用制御状態データ166はストレージ鍵データKSTRおよびメディア鍵データKMEDを用いてDESのCBCモードを利用して順に暗号化されている。ここで、記録用鍵データKSTRは、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびUMD(Mini Disc)機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データKMEDは、記録媒体にユニークなデータである。

【0213】また、署名処理部189において、SAM1051の秘密鍵データK_{SAM1}を用いて、キーファイルKF_iのハッシュ値HK_iが作成され、当該作成されたハッシュ値HK_iが、キーファイルKF_iと対応付けられてスタックメモリ200に書き込まれる。ハッシュ値HK_iは、キーファイルKF_iの作成者の正当性およびキーファイルKF_iが改竄されたか否かを検証するために用いられる。

【0214】次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図31を参照しながら説明する。この場合には、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図31に示す復号・伸長モジュール163に出力される。このとき、図31に示す相互認証部170と、図25に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。そして、復号・伸長モジュール163の復号部222において、コンテンツ

鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。このとき、課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG200、SAM1と共にEMDサービスセンタ102に送信される。

【0215】次に、図32に示すように、例えば、前述したようにネットワーク機器1601のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの購入形態を決定した後に、当該コンテンツファイルCFを格納した新たなセキヤードデータ104xを生成し、バス191を介して、AV機器1602のSAM1052にセキヤードデータ104xを転送する場合のSAM1051内での処理の流れを図33を参照しながら説明する。ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器1602に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部187に出力される。これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。また、課金処理部187は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態を示す利用制御状態データ166をEMDサービスセンタ管理部185を介してEMDサービスセンタ102に送信する。

【0216】また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図5(A)に示すコンテンツファイルCFおよびその署名データSIG_c、cpと、キーファイルKFおよびその署名データSIG_f、cpと、キーファイルKF_iおよびそのハッシュ値HK_iとをSAM管理部190に出力する。このとき、SAM1051の相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKsesによる暗号化・復号が行われる。また、署名処理部189は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データK_{SAM1}を用いて署名データSIG₄₁、SAM1を作成し、これをSAM管理部190に出力する。また、署名処理部189は、キーファイルKF_iのハッシュ値をとり、秘密鍵データK_{SAM1}を用いて署名データSIG₄₂、SAM1を作成し、これをSAM管理部190に出力する。また、SAM管理部190は、記憶データ192から、図34(D)に示す公開鍵証明書データCERcpおよびその署名データSIG₁、escと、公開鍵証明書データCERSAM1およびその署名データSIG₂、escとを読み出す。

【0217】また、相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。SAM管理部190は、図34(A)、(B)、(C)、(D)に示すデータからなる新たなセキュアコンテナ104xを生成し、暗号化・復号部171において、セッション鍵データK_{SES}を用いてセキュアコンテナ104xを暗号化した後に、図32に示すAV機器160zのSAM105₂に出力する。このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0218】以下、図32に示すように、SAM105₁から入力したセキュアコンテナ104xを、RAM型などの記録媒体(メディア)130aに書き込む際のSAM105₂内での処理の流れを、図35を参照しながら説明する。ここで、RAM型の記録媒体130aは、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

【0219】この場合には、SAM105₂のSAM管理部190は、図32および図35に示すように、ネットワーク機器160₁のSAM105₁からセキュアコンテナ104xを入力する。そして、暗号化・復号部171において、SAM管理部190を介して入力したセキュアコンテナ104xが、相互認証部170とSAM105₁の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【0220】次に、署名処理部189において、公開鍵データK_{CP}、Pを用いて、署名データSIG₆、CPの正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵データK_{SMI}、Pを用いて、署名データSIG₄₁、SAMIの正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、SAM管理部190から記録モジュール管理部855にコンテンツファイルCFが出力され、コンテンツファイルCFが図32に示すRAM型の記録媒体130aのRAM領域134に書き込まれる。

【0221】また、セッション鍵データK_{SES}を用いて復号されたキーファイルKFおよびその署名データSIG₇、CF、SIG₄₂、SAMIと、キーファイルKF₁およびそのハッシュ値HK₁と、公開鍵署名データCER_{CP}およびその署名データSIG₁、ESCと、公開鍵署名データCER_{SAMI}およびその署名データSIG₂、ESCとが、スタックメモリ200に書き込まれる。

【0222】次に、署名処理部189は、スタックメモリ200から読み出した署名データSIG₂、ESCを、記憶部192から読み出した公開鍵データK_{ESC}、Pを用いて検証して、公開鍵証明書データCER_{SAMI}の正当性を確認する。そして、署名処理部189は、公開鍵証明書データCER_{SAMI}に格納された公開鍵データK_{SAMI}、Pを用いて、スタックメモリ200に記憶されている署名データSIG₄₂、SAMIの正当性を検証する。そして、署名データSIG₄₂、SAMIが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。また、署名処理部189は、スタックメモリ200から読み出した署名データSIG₁、ESCを、記憶部192から読み出した公開鍵データK_{ESC}、Pを用いて検証して、公開鍵証明書データCER_{CP}の正当性を確認する。そして、署名処理部189は、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP}、Pを用いて、スタックメモリ200に記憶されている署名データSIG₇、SAMIの正当性を検証する。そして、署名データSIG₇、SAMIが正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。キーファイルKFの作成者および送信者が正当であることが確認されると、キーファイルKFがスタックメモリ200から読み出され、記録モジュール管理部855を介して、図34に示すRAM型の記録媒体130aのセキュアRAM領域132に書き込まれる。

【0223】また、署名処理部189は、公開鍵データK_{SAMI}、Pを用いて、ハッシュ値HK₁の正当性を検証し、キーファイルKF₁の作成者および送信者の正当性を確認する。そして、キーファイルKF₁の作成者および送信者の正当性が確認されると、図34(C)に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。なお、当該例では、キーファイルKF₁の作成者と送信元とが同じ場合を述べたが、キーファイルKF₁の作成者と送信元とが異なる場合には、キーファイルKF₁に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0224】そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を順に用いてキーファイルKF₁内のコンテンツ鍵データK_Cおよび利用制御状態データ166を暗号化して記録モジュール管理部855に出力する。そして、記録モジュール管理部855によって、暗号化されたキーファイルKF₁が、RAM型の記録媒体130aのセキュアRAM領域132に記録される。なお、メディア鍵データK

101

MEMDは、図33に示す相互認証部170と図32に示すRAM型の記録媒体1304のメディアSAM133との間の相互認証によって記憶部192に事前に記憶されている。

【0225】ここで、記録用鍵データKSTRは、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類(当該例では、AV機器1609)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データKSTRは、このような場合において、不正コピーを防止する役割を果たす。なお、本実施形態では、記録用鍵データKSTRを用いた暗号化を行わないようにしてもよい。

【0226】また、メディア鍵データKMEDは、記録媒体(当該例では、RAM型の記録媒体1304)にエンコードされたデータである。メディア鍵データKMEDは、記録媒体(当該例では、図32に示すRAM型の記録媒体1304)側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データKMEDを用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データKMEDは、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内のホストCPU810の管理外の領域に記憶されている。なお、本実施形態のように、機器側のSAM(当該例では、SAM105)とメディアSAM(当該例では、メディアSAM133)との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データKMEDを機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データKMEDを用いた暗号化および復号を行ってもよい。本実施形態では、記録用鍵データKSTRおよびメディア鍵データKMEDが、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0227】また、購入者鍵データKPINは、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データKPINは、EMDサービスセンタ102において管理される。

【0228】また、上述した実施形態では、記録モジュール260を用いて、キーファイルKF、KFをRAM型の記録媒体1304のセキュアRAM領域132に記録する場合を示したが、図32において点線で示す

102

ように、SAM1052からメディアSAM133にキーファイルKF、KFを記録するようにしてもよい。

【0229】次に、コンテンツの購入形態が未決定の図12に示すROM型の記録媒体1301をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器1602において購入形態を決定する際の処理の流れを図36および図37を参照しながら説明する。AV機器1602のSAM1052は、まず、図37に示す相互認証部170と図12に示すROM型の記録媒体1301のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データKMEDを入力する。なお、SAM1052が、事前にメディア鍵データKMEDを保持している場合には、当該入力を行わなくても良い。次に、ROM型の記録媒体1301のセキュアRAM領域132に記録されているセキュアコンテンツ104に格納された図5

(B)、(C)に示すキーファイルKFおよびその署名データSIG7、Cpと、公開鍵証明書データCERCpおよびその署名データSIG1、Rscとを、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して入力し、これをスタックメモリ200に書き込む。

【0230】次に、署名処理部189において、署名データSIG1、Rscの正当性を確認した後に、公開鍵証明書データCERCpから公開鍵データKcp、Pを取り出し、この公開鍵データKcp、Pを用いて、署名データSIG7、Cpの正当性、すなわちキーファイルKFの送信者の正当性を検証する。また、署名処理部189において、記憶部192から読み出した公開鍵データKresc、Pを用いて、キーファイルKFに格納された署名データSIG1、Rscの正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0231】署名処理部189において署名データSIG7、Cp、SIG1、Rscの正当性が確認されると、スタックメモリ200からセキュアコンテンツ番号部183に、キーファイルKFを読み出す。次に、セキュアコンテンツ番号部183において、対応する期間の配信用鍵データKD1〜KD3を用いて、キーファイルKFに格納されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテンツSDC1〜SDC3が復号され、これらがスタックメモリ200に書き込まれる。

【0232】次に、図37に示す相互認証部170と図36に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM1052の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データKcおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体1301のROM領域131から読み出したコンテンツファイルCFに格納されたコンテンツ

103

データCを図36に示す復号・伸長モジュール163に出力する。次に、復号・伸長モジュール163において、コンテンツデータCがコンテンツ鍵データKcを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、復号・伸長モジュール163からのコンテンツデータCが再生される。

【0233】次に、ユーザによる図36に示す購入形態決定操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S165が課金処理部187に入力される。

【0234】次に、課金処理部187は、操作信号S165に応じた利用制御状態データ166を作成し、これをスタックメモリ200に書き込む。次に、スタックメモリ200から暗号化・復号部173に、コンテンツ鍵データKcおよび利用制御状態データ166が出力される。

【0235】次に、暗号化・復号部173は、スタックメモリ200から入力したコンテンツ鍵データKcおよび利用制御状態データ166を、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMEMDおよび購入者鍵データKPINを用いて順次に暗号化してスタックメモリ200に書き込む。

【0236】次に、メディアSAM管理部197において、スタックメモリ200から読み出した、暗号化されたコンテンツ鍵データKcおよび利用制御状態データ166と、SAMプログラム・ダウンロード・コンテナSDC1～SDCnを用いて図34(C)に示すキーファイルKF1が生成される。また、署名処理部189において、図34(C)に示すキーファイルKF1のハッシュ値HK1が生成され、当該ハッシュ値HK1がメディアSAM管理部197に出力される。次に、図37に示す相互認証部170と図36に示すメディアSAM133との間で相互認証を行った後に、メディアSAM管理部197は、キーファイルKF1およびハッシュ値HK1を、図36に示す記録モジュール271を介してROM型の記録媒体1301のセキュアRAM領域132に書き込む。これにより、購入形態が決定されたROM型の記録媒体1301が得られる。このとき、課金処理部187が生成した利用制御状態データ166および利用履歴データ108は、所定のタイミングで、スタックメモリ200および外部メモリ201からそれぞれ読み出した後EMDサービスセンター102に送信される。なお、ROM型の記録媒体1301のメディアSAM133にキーファイルKFが格納されている場合には、図36において点線で示されるように、SAM105はメディアSAM133からキーファイルKFを入力する。また、この場合に、SAM105は、作成したキーファイルKF1をメディアSAM133に書き込む。

【0237】以下、図38に示すように、AV機器16

104

03において購入形態が未決定のROM型の記録媒体1301からセキュアコンテナ104を読み出して新たなセキュアコンテナ104yを生成し、これをAV機器1602に転送し、AV機器1602において購入形態を決定してROM型の記録媒体1305に書き込む際の処理の流れを図39、図40を参照しながら説明する。なお、ROM型の記録媒体1301からRAM型の記録媒体1305へのセキュアコンテナ104の転送は、図1に示すネットワーク機器1601およびAV機器1601～1604のいずれの間で行ってもよい。

【0238】先ず、AV機器1602のSAM105とROM型の記録媒体1301のメディアSAM133との間で相互認証を行い、ROM型の記録媒体1301のメディア鍵データKMEMD1をSAM105に転送する。また、AV機器1602のSAM105とRAM型の記録媒体1305のメディアSAM133との間で相互認証を行い、RAM型の記録媒体1305のメディア鍵データKMEMD2をSAM105に転送する。なお、メディア鍵データKMEMD1、KMEMD2を用いた暗号化をメディアSAM133およびメディアSAM133において行う場合には、メディア鍵データKMEMD1、KMEMD2の転送は行わない。

【0239】次に、SAM105は、図39に示すように、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して、ROM型の記録媒体1301のROM領域132から読み出した図5

(A)に示すコンテンツファイルCFおよびその署名データSIGa、CPと、セキュアRAM領域132から読み出した図5(B)、(C)に示すキーファイルKFおよびその署名データSIGr、cと、公開鍵証明書データCERCPおよびその署名データSIG1、ESCとを、暗号化・復号部171に出力する。また、メディアSAM管理部197から署名処理部189に、コンテンツファイルCFおよびキーファイルKFが出力される。そして、署名処理部189において、コンテンツファイルCFおよびキーファイルKFのハッシュ値がとられ、秘密鍵データKSAms、sを用いて、それぞれ署名データSIG350、SAM3、SIG352、SAM3が生成され、これらが暗号化・復号部171に出力される。また、公開鍵証明書データCERSAM3およびその署名データSIG351、ESCが記憶部192から読み出されて暗号化・復号部171に出力される。

【0240】そして、図40に示すセキュアコンテナ104yが、暗号化・復号部171においてSAM105と105との間の相互認証によって得られたセッション鍵データKsesを用いて暗号化された後に、SAM管理部190を介して、AV機器1602のSAM105xに出力される。

【0241】SAM105xでは、図41に示すよう

105

に、SAM管理部190を介してSAM105₁から入力した図40に示すセキュアコンテナ104yを暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号した後に、セキュアコンテナ104y内に格納された署名データSIG₃₅₀、CP、SIG₃₅₀、SAM₃の正当性、すなわちコンテンツファイルCFの作成者および送信者の正当性を確認する。そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、メディアSAM管理部197を介してRAM型の記録媒体130sのRAM領域134にコンテンツファイルCFが書き込まれる。

【0242】また、SAM管理部190を介してSAM105₁から入力されたキーファイルKFおよびその署名データSIG₇、CP、SIG₃₅₀、SAM₃と、公開鍵証明書データCER_{SAM3}およびその署名データSIG₃₅₁、ESCとが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号される。次に、当該復号された署名データSIG₃₅₁、ESCが、署名処理部189において署名検証され、公開鍵証明書データCER_{SAM3}の正当性が確認されると、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}を用いて、署名データSIG₇、CP、SIG₃₅₂、SAM₃の正当性、すなわちキーファイルKFの作成者および送信者の正当性が確認される。そして、キーファイルKFの作成者および送信者の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

【0243】次に、セキュアコンテナ復号部183は、対応する期間の配信用鍵データKD₁〜KD_nを用いて、キーファイルKFを復号し、当該復号したキーファイルKFをスタックメモリ200に書き込む。

【0244】次に、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。利用監視部186は、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

【0245】次に、例えば、ユーザによって試験モードが選択されると、既にセッション鍵データK_{SES}で復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データK_C、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図38に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール270において、試験モードに対応したコンテンツデータCの再生が行われる。

【0246】次に、ユーザによる図38に示す購入・利

106

用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。そして、課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。次に、コンテンツ鍵データK_Cおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MEDIA}および購入者鍵データK_{PDN}を用いて順に暗号化され、記録モジュール管理部855に出力される。そして、例えば、記録モジュール管理部855において、図34(C)に示すキーファイルKF_iが作成され、キーファイルKF_iがメディアSAM管理部197を介してRAM型の記録媒体130sのメディアSAM133に書き込まれる。また、セキュアコンテナ104yに格納されたコンテンツファイルCFは、記録モジュール管理部855によって、RAM型の記録媒体130sのRAM領域134に書き込まれる。また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

【0247】以下、SAM105₁〜105₄の実現方法について説明する。SAM105₁〜105₄の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図26に示す各機能を実現するためのセキュリティ機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0248】例えば、図26に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。また、図26に示す記憶部192や、図26に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュ・ROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁〜105₄に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。また、SA

107

M105₁～105₄には、その他に、コンテンツの利用のための有効期限や契約期間など日時検証に使用する時計機能が内蔵されている。

【0249】上述したように、SAM105₁～105₄は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105₁～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション (System Configuration) 関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリ空間を管理するMMU (Memory Management Unit) を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。また、SAM105₁～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール (ハードウェアICE、ソフトウェアICE) などを用いたリアルタイムデバッグ (リバーエンジニアリング) が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。SAM105₁～105₄自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0250】SAM105₁～105₄の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにみ解読することが可能となる仕掛けをする場合とがある。前者は、暗号ライブラリーモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタソフトウェアと呼ばれるもので、ICE (デバッグ) で実行状況を解読されても、そのタスクの実行順序がバラバラであったり (この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う)、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ (Min: OS) と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

108

【0251】次に、図25に示す復号・伸長モジュール163について説明する。図25に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。相互認証部220は、復号・伸長モジュール163がSAM105₁からデータを入力する際に、図32に示す相互認証部170との間で相互認証を行ってセッション鍵データKsesを生成する。

【0252】復号部221は、SAM105₁から入力したコンテンツ鍵データKc、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データKsesを用いて復号する。そして、復号部221は、復号したコンテンツ鍵データKcおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0253】復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データKcを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0254】伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。伸長部223は、例えば、図5(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0255】電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。このように、ユーザ電子透かし情報は、コンテンツデータCを再生すると共に、復号・伸長モジュール163において埋め込まれる。なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0256】半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試験時の再生機能を限定したり、試験可能な期間を限定するなどの制御を行う。

【0257】再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0258】次に、コンテンツプロバイダ101、EM

Dサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを受送信する際のデータフォーマットについて説明する。図42(A)は、コンテンツプロバイダ101からSAM1051にデータ1051をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod50が送信される。モジュールMod50には、モジュールMod51およびその秘密鍵データKcp、sによる署名データSIGcpが格納されている。モジュールMod51には、コンテンツプロバイダ101の秘密鍵データKcp、pを格納した公開鍵証明書データCERcpと、公開鍵証明書データCERcpに対しての秘密鍵データKres、sによる署名データSIGresと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERcpを格納したモジュールMod50を、コンテンツプロバイダ101からSAM1051に送信することで、SAM1051において署名データSIGcpの検証を行なう際に、EMDサービスセンタ102からSAM1051に公開鍵証明書データCERcpを送信する必要がなくなる。

【0259】図42(B)、(C)は、コンテンツプロバイダ101からSAM1051にデータDataをアウト・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からSAM1051に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図42(B)に示すモジュールMod52が送信される。モジュールMod52には、送信するデータDataと、その秘密鍵データKcp、sによる署名データSIGcpとが格納されている。また、EMDサービスセンタ102からSAM1051には、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図42(C)に示すモジュールMod53が送信される。モジュールMod53には、コンテンツプロバイダ101の公開鍵証明書データCERcpと、その秘密鍵データKres、sによる署名データSIGresとが格納されている。

【0260】図42(D)は、SAM1051からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセ

ッション鍵データKsesで暗号化したモジュールMod54が送信される。モジュールMod54には、モジュールMod55およびその秘密鍵データKcp、sによる署名データSIGcpが格納されている。モジュールMod55には、SAM1051の秘密鍵データKcp、pを格納した公開鍵証明書データCERcpと、公開鍵証明書データCERcpに対しての秘密鍵データKres、sによる署名データSIGresと、送信するデータDataとが格納されている。このように、公開鍵証明書データCERcpを格納したモジュールMod55を、SAM1051からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIGcpの検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCERcpを送信する必要がなくなる。

【0261】図42(E)、(F)は、SAM1051からコンテンツプロバイダ101にデータDataをアウト・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図42(E)に示すモジュールMod56が送信される。モジュールMod56には、送信するデータDataと、その秘密鍵データKcp、sによる署名データSIGcpとが格納されている。また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データKsesで暗号化した図42(F)に示すモジュールMod57が送信される。モジュールMod57には、SAM1051の公開鍵証明書データCERcpと、その秘密鍵データKres、sによる署名データSIGresとが格納されている。

【0262】図43(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod58が送信される。モジュールMod58には、モジュールMod59およびその秘密鍵データKcp、sによる署名データSIGcpが格納されている。モジュールMod59には、コンテンツプロバイダ101の秘密鍵データKcp、pを格納した公開鍵証明書データCERcpと、公開鍵証明書データCERcpに対しての秘密鍵データKres、sによる署名データSIGresと、送信す

III

るデータDataとが格納されている。

【0263】図43 (I)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データKsesで暗号化した図43 (H)に示すモジュールMod63が送信される。モジュールMod63には、送信するデータDataと、その秘密鍵データKcp、sによる署名データSIGcpとが格納されている。このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データCERcpは既に登録されている。

【0264】図43 (I)は、SAM1051からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化したモジュールMod63が送信される。モジュールMod63には、モジュールMod63およびその秘密鍵データKksami、sによる署名データSIGksamiが格納されている。モジュールMod62には、SAM1051の秘密鍵データKksami、pを格納した公開鍵証明書データCERksamiと、公開鍵証明書データCERksamiに対しての秘密鍵データKresc、sによる署名データSIGrescと、送信するデータDataとが格納されている。

【0265】図43 (J)は、SAM1051からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、SAM1051からEMDサービスセンタ102に、EMDサービスセンタ102とSAM1051との間の相互認証によって得たセッション鍵データKsesで暗号化した図43 (J)に示すモジュールMod63が送信される。モジュールMod63には、送信するデータDataと、その秘密鍵データKksami、sによる署名データSIGksamiとが格納されている。このとき、EMDサービスセンタ102にはSAM1051の公開鍵証明書データCERksamiは既に登録されている。

【0266】以下、SAM1051～1054の出荷時に示すEMDサービスセンタ102への登録処理について説明する。なお、SAM1051～1054の登録処理は同じであるため、以下、SAM1051の登録処理について述べる。SAM1051の出荷時には、図24に示すEMDサービスセンタ102の鍵サーバ141

I12

によって、SAM管理部149を介して、図26などに示す記憶部192に以下に示す鍵データが初期登録される。また、SAM1051に、例えば、出荷時に、記憶部192などに、SAM1051がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部192には、例えば、図30において左側に「*」が付されているSAM1051の識別子SAM_ID、記録用鍵データKSTR、ルート認証局2の公開鍵データKrc-a、EMDサービスセンタ102の公開鍵データKresc、p、SAM1051の秘密鍵データKksami、s、公開鍵証明書データCERksamiおよびその署名データSIGresc、s、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データCERksamiは、SAM1051を出荷後に登録する際にEMDサービスセンタ102からSAM1051に送信してもよい。

【0267】また、記憶部192には、SAM1051の出荷時に、図5に示すコンテンツファイルCFおよびキーファイルKFを読み込み形式を示すファイルリダが、EMDサービスセンタ102によって書き込まれる。SAM1051では、コンテンツファイルCFおよびキーファイルKFに格納されたデータを利用する際に、記憶部192に記憶されたファイルリダが用いられる。

【0268】ここで、ルート認証局2の公開鍵データKrc-aは、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データKrc-aは、図1に示すルート認証局2によって発行される。また、EMDサービスセンタ102の公開鍵データKresc、pは、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データKresc、pは192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データKresc、pを登録する。また、ルート認証局92は、公開鍵データKresc、pの公開鍵証明書データCERrescを作成する。公開鍵データKresc、pを格納した公開鍵証明書データCERrescは、好ましく、SAM1051の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データCERrescは、ルート認証局92の秘密鍵データKroott、sで署名されている。

【0269】EMDサービスセンタ102は、乱数を発生してSAM1051の秘密鍵データKksami、s、を生成し、これとペアとなる公開鍵データKksami、pを生成する。また、EMDサービスセンタ102は、ルート認証局92の認証をもって、公開鍵

データK_{SAM1}、Pの公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データK_{ESC}、Sを用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

【0270】また、SAM1051には、図24に示すEMDサービスセンタ102のSAM管理部149により、EMDサービスセンタ102の管理下にある一意（ユニーク）な識別子SAM_IDが割り当てられ、これがSAM1051の記憶部192に格納されると共に、図24に示すSAMデータベース149aにも格納される。EMDサービスセンタ102によって管理される。

【0271】また、SAM1051は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データKD1〜KD3が転送される。すなわち、SAM1051を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM1051を搭載している機器（当該例では、ネットワーク機器1601）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。SAM1051は、上述した登録手続を経た後でないと使用できない。

【0272】EMDサービスセンタ102は、SAM1051のユーザによる登録手続に応じて、ユーザに固有の識別子USER_IDを発行し、例えば、図24に示すSAMデータベース149aにおいて、SAM_IDとUSER_IDとの対応関係を管理し、購読時に利用する。また、EMDサービスセンタ102は、SAM1051のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【0273】次に、図30に示すように、SAM1051内の記憶部192にSAM登録リストを格納する手順について説明する。図1に示すSAM1051は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されたトポロジーマップを利用して、自分の系に存在するSAM1052〜SAM1054のSAM登録リストを得る。なお、IEEE1394シリアルバスであ

るバス191に応じて生成されたトポロジーマップは、例えば、図44に示すように、バス191にSAM1051〜1054に加えてAV機器1601、1602のSCMS処理回路1051、1052が接続されている場合に、SAM1051〜1054およびSCMS処理回路1051、1052を対象として生成される。従って、SAM1051は、当該トポロジーマップから、SAM1051〜1054についての情報を抽出して図45に示すSAM登録リストを生成する。

【0274】そして、SAM1051は、図45に示すSAM登録リストを、EMDサービスセンタ102に登録して署名を得る。これらの処理は、バス191のセッションを利用してSAM1051が自動的に、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。EMDサービスセンタ102は、SAM1051から図45に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM1051より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションタグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。また、EMDサービスセンタ102は、決済時にはSAM1051に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。これにより、図46に示すSAM登録リストが作成される。なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションタグによって、当該SAMの有効および無効を示している。

【0275】以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。図47は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データK_{CPR}、Pの公開鍵証明書CER_{CPR}をコンテンツプロバイダ101に送信する。また、EMDサービスセンタ102は、SAM1051〜1054が所定の登録処理を経た後に、SAM1051〜1054の公開鍵データK_{SAM1}、P〜K_{SAM4}、Pの公開鍵証明書CER_{CPR1}〜CER_{CPR4}をSAM1051〜1054に送信する。また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1か月の3か月分の配

115

信用鍵データKD₁～KD₃をユーザホームネットワーク103のSAM105₁～105₄に送信する。このように、EMDシステム100では、配信用鍵データKD₁～KD₃を予めSAM105₁～105₄に配給しているため、SAM105₁～105₄とEMDサービスセンタ102との間がオフラインの状態でも、SAM105₁～105₄においてコンテンツプロバイダ101から配給されたセキュアコンテナ104を符号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記録され、利用履歴データ108は、SAM105₁～105₄とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リポーションリストで無効の対象とする。なお、利用制御状態データ166は、原則として、リアルタイムで、SAM105₁～105₄からEMDサービスセンタ102に送信される。

【0276】ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図18に示す登録用モジュールMod₂を、EMDサービスセンタ102に送信する。そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して格納化する。また、EMDサービスセンタ102は、登録用モジュールMod₂に応じた6カ月のキーファイルKFを作成し、これをコンテンツプロバイダ101に送信する。

【0277】ステップS3：コンテンツプロバイダ101は、図5(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG_s、cpと、キーファイルKFおよびその署名データSIG_k、cpとを作成し、これらと図5(C)に示す公開鍵証明書データCER_{pub}およびその署名データSIG₁、rscとを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、ユーザホームネットワーク103のSAM105₁～105₄に配給する。オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で(すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして)、セキュアコンテナ104がコンテンツプロバイダ101からユーザホームネットワーク103に配送される。また、オフラインの場合には、ROM型あるいはRAM型の記録媒体に記録された状態で、セキュアコンテナ104が、コンテンツプロバイダ101からユーザホームネットワーク103に配送される。

【0278】ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、コンテン

116

ツプロバイダ101から配給を受けたセキュアコンテナ104内の署名データSIG_s、cp、SIG_k、cp、SIG₁、rscを検証して、コンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認した後に、対応する期間の配信用鍵データKD₁～KD₃を用いてキーファイルKFを復号する。

【0279】ステップS5：SAM105₁～SAM105₄において、ユーザによる図25に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。このとき、図31に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

【0280】ステップS6：SAM105₁～SAM105₄の図31に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0281】ステップS7：EMDサービスセンタ102は、図24に示す決済処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG_{pub}を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0282】ステップS8：決済機関91において、署名データSIG_{pub}の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0283】以上説明したように、EMDシステム100では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105₁～105₄内で行う。また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信用鍵データKD₁～KD₃を用いて暗号化されており、配信用鍵データKD₁～KD₃を保持しているSAM105₁～105₄内でのみ復号される。そして、SAM105₁～105₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。従って、EMDシステム100によれば、ユーザホームネッ

117

トワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

【0284】また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配信を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁~105₄におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

【0285】また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂~160₄においてコンテンツデータCを購入、利用、記録および伝送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0286】図48は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。図48に示すように、マルチプロセッサシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを伝送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを伝送するプロトコルとして例えば1394シリアルバス・インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

【0287】第1実施形態の第1変形例

上述した実施形態では、図5(B)に示すように、EMDサービスセンタ102において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁~105₄において配信用鍵データKDを用いてキーファイルKFを復号する場合を示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁~105₄にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータCを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。但し、上述した第1実施形態の場合でも、

118

配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【0288】また、上述した実施形態では、図5(B)に示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP(プライスタグデータ)を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データK_{cp}を用いて作成した署名データを添付する。

【0289】第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を示したが、例えば、図49に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求データ152を送信し、コンテンツプロバイダ101自らが、決済請求データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

【0290】第1実施形態の第3変形例

上述した第1実施形態では、単一のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁~105₄に、セキュアコンテナ104を供給する場合を示したが、2以上のコンテンツプロバイダ101a、101bからSAM105₁~105₄にそれぞれセキュアコンテナ104a、104bを供給するようにしてもよい。図50は、コンテンツプロバイダ101a、101bを用いる場合の第1実施形態の第3変形例に係わるEMDシステムの構成図である。この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれの6カ月分の配信用鍵データKD_{a1}~KD_{a6}およびKD_{b1}~KD_{b6}を用いて暗号化したキーファイルKF_{a1}~KF_{a6}およびKF_{b1}~KF_{b6}を配信する。また、EMDサービスセンタ102は、SAM105₁~105₄に、3カ月分の配信用鍵データKD_{a1}~KD_{a3}およびKD_{b1}~KD_{b3}を配信する。

【0291】そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データK_{ca}を用いて暗号化したコンテンツファイルCF_aと、EMDサービスセンタ102から受信した対応する期間のキーファイルKF_{a1}~KF_{a6}とを格納したセキュアコンテナ104aをSAM105₁~105₄にオンラインおよび/またはオフラインで供給する。このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子コンテンツIDが用いられ、EMDサービスセンタ102によって、コンテンツデータが

一元的に管理される。また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKc bを用いて暗号化したコンテンツファイルCF bと、EMDサービスセンタ102から受信した対応する期間のキーファイルKF b1~KF b6とを格納したセキュアコンテナ104bをSAM1051~1054にオンラインおよび/またはオフラインで供給する。

【0292】SAM1051~1054は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKDa1~KDa5を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。また、SAM1051~1054は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKDb1~KDb5を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

【0293】EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

【0294】また、EMDサービスセンタ102は、権利書データ106a、106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a、106bに対応するキーファイルKF a、KF bに対して、グローバルユニークな識別子コンテンツIDを配付する。また、EMDサービスセンタ102は、コンテンツプロバイダ101a、101bの公開鍵証明書データCERa、CERbを発行し、これに自らの署名データSIGa、esc、SIGb、escを付してその正当性を認証する。

【0295】第1実施形態の第4変形例

上述した実施形態では、コンテンツファイルCFおよびキーファイルKFをディレクトリ構造でセキュアコンテナ104内に格納してコンテンツプロバイダ101からSAM1051~1054に送信する場合を例示したが、コンテンツファイルCFおよびキーファイルKFを、別々にSAM1051~1054に送信してもよい。これには、例えば、以下に示す第1の手法と第2の手法とがある。第1の手法では、図51に示すように、コンテンツプロバイダ101からSAM1051~1054に、通信プロトコルに依存しない形式で、コンテ

ツファイルCFおよびキーファイルKFを別々に送信する。また、第2の手法では、図52に示すように、コンテンツプロバイダ101からSAM1051~1054にコンテンツファイルCFを通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102からSAM1051~1054にキーファイルKFを送信する。当該キーファイルKFの送信は、例えば、SAM1051~1054のユーザが、コンテンツデータCの購入形態を決定しようとするときに、EMDサービスセンタ102からSAM1051~1054に送信される。上述した第1の手法および第2の手法を採用する場合には、関連するコンテンツファイルCF相互間と、コンテンツファイルCFとそれに対応するキーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータを用いてリンク関係を確立する。SAM1051~1054では、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5(A)、(B)に示すものが採用される。また、この場合に、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データSIGa、cp、SIGb、cpを送信することが好ましい。

第1実施形態の第5変形例

上述した実施形態では、セキュアコンテナ104内において、コンテンツファイルCFおよびキーファイルKFを別々に設けた場合を例示したが、例えば、図53に示すように、セキュアコンテナ104内において、コンテンツファイルCF内にキーファイルKFを格納するようにしてもよい。この場合に、キーファイルKFを格納したコンテンツファイルCFに対して、コンテンツプロバイダ101の秘密鍵データKcr、sによる署名データが付けられる。

第1実施形態の第6変形例

上述した実施形態では、コンテンツデータCをコンテンツファイルCFに格納し、コンテンツ鍵データKcおよび権利書データ106をキーファイルKF内に格納してコンテンツプロバイダ101からSAM1051などに送信する場合を例示したが、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ101からSAM1051などに、通信プロトコルに依存しない形式で送信してもよい。

【0296】例えば、図54に示すように、コンテンツプロバイダ101において、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFを格納したセキュアコンテナ104sを作成し、セキュアコンテナ104s

121

をSAM105などに通信プロトコルに依存しない形式で送信してもよい。

【0297】また、図55に示すように、コンテンツプロバイダ101からSAM105などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106を含むキーファイルKFとを通信プロトコルに依存しない形式で個別に送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと同一経路で送信する。

【0298】また、図56に示すように、コンテンツプロバイダ101からSAM105などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信すると共に、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106を含むキーファイルKFをEMDサービスセンタ102からSAM105などに送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと別経路で送信する。

【0299】また、図57に示すように、コンテンツプロバイダ101からSAM105などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、同一経路で送信する。

【0300】また、図58に示すように、コンテンツプロバイダ101からSAM105などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCを、通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102からSAM105などにコンテンツ鍵データKcおよび権利書データ106を送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、別経路で送信する。

【0301】第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105へ105にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0302】図59は、本実施形態のEMDシステム300の構成図である。図59に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。コンテンツプロ

122

バイダ301、EMDサービスセンタ302、SAM305、サービスプロバイダ310は、それぞれ請求項22などに係るデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505、サービスプロバイダ310に加えて、サービスプロバイダ310に対して認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。また、ユーザホームネットワーク303は、ネットワーク機器360およびAV機器360を有している。ネットワーク機器360はSAM305およびCAモジュール311を内蔵しており、AV機器360はそれぞれSAM305、サービスプロバイダ310からセキュアコンテンツ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行う点とを除いて、前述した第1実施形態のSAM105に105と同じである。

【0303】先ず、EMDシステム300の概要について説明する。EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書（UCP：Usage Control Policy）データ106およびコンテンツ鍵データKcを、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106およびコンテンツ鍵データKcは、EMDサービスセンタ302に登録されて権威化（認証）される。

【0304】また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納した図5に示すセキュアコンテンツ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどで

123

サービスプロバイダ310に供給する。また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0305】サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なう。セキュアコンテナ104の作成者および送信者の確認する。次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格（SRP）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（PT）312を作成する。そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データK_{SP}による署名データとを格納したセキュアコンテナ304を作成する。このとき、キーファイルKFは、配信用鍵データKD₁～KD₆によって暗号化されており、サービスプロバイダ310は当該配信用鍵データKD₁～KD₆を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。また、EMDサービスセンタ302は、プライスタグデータ312を登録して増成化する。

【0306】サービスプロバイダ310は、オンラインおよび/またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に供給する。このとき、オフラインの場合には、セキュアコンテナ304はROM型の記録媒体などに記録されてSAM3051～3054にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データK_{SES}を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データK_{SES}を用いて復号した後に、SAM3051～3054に転送する。この場合に、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を送信する通信プロトコルとして、デジタル放送であればMPEG（Multimedia and Hypermedia information coding Experts Group）プロトコルが用いられ、インターネットであればXML/SMIL/HTML（HyperText Markup Language）（用いられ、これらの通信プロトコル内に、セキュアコンテナ304が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。従って、通信プロトコルとセキュアコンテナ304との間でフォーマットの整合

124

性をとる必要性はなく、セキュアコンテナ304のフォーマットを柔軟に設定できる。

【0307】次に、SAM3051～3054において、セキュアコンテナ304内に格納された署名データを検証して、セキュアコンテナ304に格納されたコンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認する。そして、SAM3051～3054において、当該正当性が確認されると、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD₆を用いてキーファイルKFを復号する。SAM3051～3054に供給されたセキュアコンテナ304は、ネットワーク機器3601およびAV機器3602～3604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM3051～3054は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴（Usage Log）データ308として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。また、SAM3051～3054は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御状態データ（UCS: Usage control state Data）166をEMDサービスセンタ302に送信する。

【0308】EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った全額が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

【0309】本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンダリ認証局（Secondary Certificate Authority）としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106、コンテンツ鍵データKcおよびサービスプロ

バイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。また、EMDサービスセンタ302は、例えば、配信鍵データKDa〜KDaなどの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM3051〜SAM3054から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機能を有する。

【0310】以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

【コンテンツプロバイダ301】図60は、コンテンツプロバイダ301の機能ブロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。図60に示すように、コンテンツプロバイダ301は、コンテンツマスタースデータベース111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、署名処理部117、セキュアコンテンツ作成部118、セキュアコンテンツデータベース118a、キーマイルデータベース118b、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、EMDサービスセンタ管理部125およびサービスプロバイダ管理部324を有する。

【0311】図60において、図3と同一符号を付した構成要素は、前述した第1実施形態において図3および図4を参照しながら説明した同一符号の構成要素と同じである。すなわち、コンテンツプロバイダ301は、図3に示すSAM管理部124の代わりにはサービスプロバイダ管理部324を設けた構成をしている。サービスプロバイダ管理部324は、セキュアコンテンツ作成部118から入力した図5に示すセキュアコンテンツ104を、オフラインおよび/またはオンラインで、図59に示すサービスプロバイダ310に提供する。

【0312】サービスプロバイダ管理部324は、図5に示すセキュアコンテンツ104をオンラインでサービスプロバイダ310に配信する場合には、暗号化・復号部121においてセッション鍵データKsesを用いてセキュアコンテンツ104を暗号化した後に、ネットワークを介してサービスプロバイダ310に配信する。

【0313】また、図4に示したコンテンツプロバイダ301内でのデータの流れは、コンテンツプロバイダ301にも同様に適用される。

【0314】以下、コンテンツプロバイダ301からサービスプロバイダ310にセキュアコンテンツ104を送

信する際の処理の流れを説明する。図61および図62は、コンテンツプロバイダ301からサービスプロバイダ310にセキュアコンテンツ104を送信する際の処理の流れを示すフローチャートである。

ステップC1：コンテンツプロバイダ301とサービスプロバイダ310との間で相互認証を行う。

ステップC2：ステップC1の相互認証によって得られたセッション鍵データKsesを、コンテンツプロバイダ301およびサービスプロバイダ310の間で共有する。

ステップC3：サービスプロバイダ310によって、コンテンツプロバイダ301が所有する（CP用）セキュアコンテンツデータベース118aにアクセスが行われる。

ステップC4：サービスプロバイダ310は、例えば、セキュアコンテンツデータベース118aにおいて一元的に管理されているコンテンツIDとメタデータとのリストを参照して自らの配信サービスに必要なセキュアコンテンツ104を選択する。

【0315】ステップC5：コンテンツプロバイダ301は、ステップC4で選択したセキュアコンテンツ104を、ステップC2で共有したセッション鍵データKsesを用いて暗号化する。

ステップC6：コンテンツプロバイダ301は、ステップC5で得られたセキュアコンテンツ104を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

【0316】ステップC7：サービスプロバイダ310は、ダウンロードを行う。

ステップC8：サービスプロバイダ310は、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテンツ104を取り出す。

ステップC9：サービスプロバイダ310は、セキュアコンテンツ104を、ステップC2で共有したセッション鍵データKsesを用いて復号する。

ステップC10：サービスプロバイダ310は、復号したセキュアコンテンツ104に格納されている署名データを検証して、送信者の正当性を確認し、送信者が正当であることの確認を条件にステップC11の処理を行う。

ステップC11：サービスプロバイダ310は、セキュアコンテンツ104を自らのセキュアコンテンツデータベースに格納する。

【0317】【サービスプロバイダ310】サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテンツ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテンツ304を作成し、ユーザホームネットワーク303のネットワーク機器360およびAV機器360a〜360iにセキュアコンテンツ304をオンラインおよび/またはオフラインで配信する。サービスプロバイダ310

127

によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0318】図63は、サービスプロバイダ310の機能ブロック図である。なお、図63には、コンテンツプロバイダ301から供給を受けたセキュアコンテンツ104を用いて作成したセキュアコンテンツ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。図63に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテンツ作成部355、セキュアコンテンツデータベース355a、ブライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

【0319】以下、コンテンツプロバイダ301から供給を受けたセキュアコンテンツ104からセキュアコンテンツ304を作成し、これをユーザホームネットワーク303に供給する際のサービスプロバイダ310内での処理の流れを図63および図64を参照しながら説明する。図64は、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテンツ304を供給する処理を説明するためのフローチャートである。<ステップD1>コンテンツプロバイダ管理部350は、オンラインおよび/またはオフラインで、コンテンツプロバイダ301から図5に示すセキュアコンテンツ104の供給を受けてセキュアコンテンツ104を記憶部351に書き込む。このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図60に示す相互認証部120と図63に示す相互認証部352との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテンツ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。なお、サービスプロバイダ310は、記憶部351とは別に、セキュアコンテンツ104を格納するための専用のセキュアコンテンツデータベースを有してもよい。

【0320】<ステップD2>次に、署名処理部354において、記憶部351に記憶されているセキュアコンテンツ104の図5（C）に示す署名データSIG₁、ESC記憶部351から読み出したEMDサービスセンタ302の公開鍵データK_{ESC}、Pを用いて検証し、その正当性が認められた後に、図5（C）に示す公

128

開鍵証明書データCER_{CP}から公開鍵データK_{CP}、Pを取り出す。次に、署名処理部354は、当該取り出した公開鍵データK_{CP}、Pを用いて、記憶部351に記憶されているセキュアコンテンツ104の図5（A）、（B）に示す署名データSIG_G、CP、SIG_G、CPの検証、すなわちコンテンツファイルCFの作成者および送信者と、キーファイルKFの送信者との正当性の検証を行う。また、署名処理部354は、記憶部351から読み出した公開鍵データK_{ESC}、Pを用いて、図5（B）に示すキーファイルKFに格納された署名データSIG_{K1}、ESCの検証、すなわちキーファイルKFの作成者の正当性の検証を行う。このとき、署名データSIG_{K1}、ESCの検証は、キーファイルKFがEMDサービスセンタ302に登録されているか否かの検証も兼ねている。

【0321】<ステップD3>次に、セキュアコンテンツ作成部355は、署名データSIG_G、CP、SIG_G、CP、SIG_{K1}、ESCの正当性が確認されると、記憶部351からコンテンツファイルCFおよびその署名データSIG_G、CPと、キーファイルKFおよびその署名データSIG_G、CPと、サービスプロバイダ310の公開鍵証明書データCER_{SP}およびその署名データSIG_{K1}、ESCとを読み出す。

【0322】また、ブライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格をすブライスタグデータ312を作成し、記憶部351に記憶する。

【0323】また、署名処理部354は、コンテンツファイルCF、キーファイルKFおよびブライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データK_{SP}、Pを用いて、署名データSIG_G、SP、SIG_G、SP、SIG_G、SP、SIG_G、SPを作成し、これをセキュアコンテンツ作成部355に出力する。ここで、署名データSIG_G、SPはコンテンツファイルCFの送信者の正当性を検証するために用いられ、署名データSIG_G、SPはブライスタグデータ312の作成者および送信者の正当性を検証するために用いられる。署名データSIG_G、SPはキーファイルKFの送信者の正当性を検証するために用いられ、署名データSIG_G、SPはブライスタグデータ312の作成者および送信者の正当性を検証するために用いられる。

【0324】次に、セキュアコンテンツ作成部355は、図65（A）～（D）に示すように、コンテンツファイルCFおよびその署名データSIG_G、CP、SIG_G、CP、SIG_{K1}、ESCと、キーファイルKFおよびその署名データSIG_G、CP、SIG_G、CP、SIG_{K1}、ESCと、ブライスタグデータ312およびその署名データSIG_G、SPと、公開鍵証明書データCER_{SP}およびそ

129

の署名データSIG_{sl}、ESCと、公開鍵証明書データCER_{cr}およびその署名データSIG_{cr}、ESCとを格納したセキュアコンテンツ304を作成し、セキュアコンテンツデータベース355aに格納する。セキュアコンテンツ304は、例えば、コンテンツIDなどを用いてサービスプロバイダ310によって一元的に管理される。

【0325】<ステップD4>セキュアコンテンツ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテンツ304をセキュアコンテンツデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。このとき、セキュアコンテンツ304は、複数のコンテンツツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテンツであってよい。例えば、単数のセキュアコンテンツ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツツファイルCFを単独のセキュアコンテンツ304に格納してもよい。これらの複数のコンテンツツファイルCFなどは、ディレクトリ構造でセキュアコンテンツ304内に格納してもよい。

【0326】また、セキュアコンテンツ304は、デジタル放送で送信される場合には、MHEG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML (Hyper Text Markup Language) プロトコルが用いられる。このとき、セキュアコンテンツ304内のコンテンツツファイルCFおよびキーファイルKFなどは、MHEGおよびHTMLのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ310とユーザホームネットワーク303との間で採用される通信プロトコル内の所定の階層に格納される。

【0327】例えば、セキュアコンテンツ304をデジタル放送で送信する場合には、図6に示すように、コンテンツツファイルCFが、MHEGオブジェクト (Object) 内のMHEGコンテンツデータとして格納される。また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES (Packetized Elementary Stream) - Videoに格納され、音声である場合にはPES - Audioに格納され、静止画である場合にはPrivate-Dataに格納される。また、図6に示すように、キーファイルKF、ブライスタグデータ312および公開鍵証明書データCER_{cr}、CER_{st}は、トランスポート層プロトコルのTS Packet内のECM (Entitlement Control Message) に格納される。ここで、コンテン

130

ツファイルCF、キーファイルKF、ブライスタグデータ312および公開鍵証明書データCER_{cr}、CER_{st}は、コンテンツツファイルCFのヘッダ内のディレクトリ構造データDSD1によって相互間のリンクが確立されている。

【0328】次に、ユーザホームネットワーク管理部357は、セキュアコンテンツ304を、オフラインおよび/またはオンラインでユーザホームネットワーク303に供給する。ユーザホームネットワーク管理部357は、セキュアコンテンツ304をオンラインでユーザホームネットワーク303のネットワーク機器360に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データK_{ses}を用いてセキュアコンテンツ304を暗号化した後に、ネットワークを介してネットワーク機器360に配信する。

【0329】なお、ユーザホームネットワーク管理部357は、セキュアコンテンツ304を例えば衛星などを介して放送する場合には、セキュアコンテンツ304をスクランブル鍵データK_{scr}を用いて暗号化する。また、スクランブル鍵データK_{scr}をワーク鍵データK_wを暗号化し、ワーク鍵データK_wをマスタ鍵データK_mを用いて暗号化する。そして、ユーザホームネットワーク管理部357は、セキュアコンテンツ304と共に、スクランブル鍵データK_{scr}およびワーク鍵データK_wを、衛星を介してユーザホームネットワーク303に送信する。また、例えば、マスタ鍵データK_mを、ICカードなどに記憶してオフラインでユーザホームネットワーク303に供給する。

【0330】また、ユーザホームネットワーク管理部357は、ユーザホームネットワーク303から、当該サービスプロバイダ310が配給したコンテンツデータCに關してのSP用購入履歴データ309を受信すると、これを記憶部351に書き込む。サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購入履歴データ309を参照する。また、ユーザ嗜好フィルタ生成部920は、SP用購入履歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM3051~3054のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク管理部357を介してユーザホームネットワーク303のCAMモジュール311に送信する。

【0331】図68には、サービスプロバイダ310内におけるEMDサービスセンタ302との間の通信に関連するデータの流れが示されている。なお、以下に示す処理を行う前提として、サービスプロバイダ310の関係者は、例えば、自らの身元証明書を必ず決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。識別子SP_IDは、記憶部351に記憶される。

131

【0332】先ず、サービスプロバイダ310が、EMDサービスセンタ302に、自らの秘密鍵データK_{SP, S}に対応する公開鍵データK_{SP, S}の正当性を証明する公開鍵証明書データCER_{SP, S}を要求する場合の処理を図68を参照しながら説明する。サービスプロバイダ310は、真性乱数発生器を用いて乱数を発生して秘密鍵データK_{SP, S}を生成し、当該秘密鍵データK_{SP, S}に対応する公開鍵データK_{SP, P}を作成して記憶部351に記憶する。EMDサービスセンタ管理部358、サービスプロバイダ310の識別子SP_IDおよび公開鍵データK_{SP, P}を、EMDサービスセンタ302に送信する。そして、EMDサービスセンタ管理部348は、当該登録に応じて、公開鍵証明書データCER_{SP, S}およびその署名データSIG_{SP, S}をEMDサービスセンタ302から入力して記憶部351に書き込む。

【0333】次に、サービスプロバイダ310が、EMDサービスセンタ302にブライスタグデータ312を登録して権威化する場合の処理を図68を参照して説明する。

【0334】この場合には、署名処理部354において、記憶部351から読み出したブライスタグデータ312およびグローバルユニークな識別子であるコンテンツIDを格納した図69に示すモジュールMod_{ios}のハッシュ値が求められ、秘密鍵データK_{SP, S}を用いて署名データSIG_{io, SP}が生成される。また、記憶部351から公開鍵証明書データCER_{SP, S}およびその署名データSIG_{SP, S}が読み出される。そして、図69に示すブライスタグ登録要求用モジュールMod_{io2}が、相互認証部352とEMDサービスセンタ302との間の相互認証によって得られたセッション鍵データK_{SP, S}を用いて暗号化し、サービスプロバイダ310のグローバルユニークな識別子SP_IDを格納してよい。

【0335】また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信した決済レポートデータ307sを記憶部351に書き込む。

【0336】また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信したマーケティング情報データ904を記憶部351に記憶する。マーケティング情報データ904は、サービスプロバイダ310が今後供給するコンテンツデータCを決定する際に参考される。

【0337】[EMDサービスセンタ302] EMDサービスセンタ302は、前述したように、認証局(C

132

A: Certificate Authority)、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。図70は、EMDサービスセンタ302の機能の構成図である。図70に示すように、EMDサービスセンタ302は、鍵サーバ141、鍵データベース141a、KF作成部153、決済処理部442、署名処理部443、決算機関管理部144、証明書・権利書管理部445、権利書データベース445a、証明書データベース445b、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151、サービスプロバイダ管理部390、SPデータベース390a、コンテンツID作成部851、ユーザ嗜好フィルタ生成部901およびマーケティング情報データ生成部902を有する。図70において、図23および図24と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと略同機能を有している。

【0338】以下、図70において、新たな符号を付した機能ブロックについて説明する。なお、図70には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。また、図71には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ301との間で送受信されるデータに関連するデータの流れが示されている。また、図72には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、図59に示すSAM3051〜3054および決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0339】決算処理部442は、図72に示すように、SAM3051〜3054から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびブライスタグデータ312に基づいて決済処理を行う。なお、この際、決済処理部442は、サービスプロバイダ310によるダンピングの有無などを監視する。決済処理部442は、決済処理により、図72に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。また、決済処理により、図70および図72に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。ここで、決済請求権データ152c、152sは、当該データに基づいて、決済機関91に全線の

133

支払いを請求できる権威化されたデータである。

【0340】ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図73に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子であるコンテンツID、セキュアコンテナ304に格納されたコンテンツデータCを提供したコンテンツプロバイダ301の識別子CPID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SPID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子MediaID、セキュアコンテナ304を配給を受けたSAM3051〜3054の識別子SAMID、当該SAM1051〜1054のユーザのUSERIDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【0341】証明書・権利書管理部445は、証明書データベース445bに登録されて権威化された公開鍵証明書データCER、公開鍵証明書データCERs、および公開鍵証明書データCERsami〜CERsam2などを読み出すと共に、権利書データベース445aにコンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKc、並びにサービスプロバイダ310のプライスタグデータ312などを登録して権威化する。このとき、証明書・権利書管理部445は、権利書データ106、コンテンツ鍵データKcおよびプライスタグデータ312などのハッシュ値をとり、秘密鍵データKescを用いた署名データを付して権威化証明書データを作成する。

【0342】コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されているコンテンツプロバイダ101の識別子CPIDなどを管理するCPデータベース148aにアクセスできる。

【0343】ユーザ嗜好フィルタ生成部901は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM3051〜3054のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM3051〜3054

134

に送信する。

【0344】マーケティング情報データ生成部902は、利用履歴データ308に基づいて、例えば、複数のサービスプロバイダ310によってユーザホームネットワーク103に供給されたコンテンツデータCの全体の購入状況などを示すマーケティング情報データ904を生成し、これをサービスプロバイダ管理部390を介して、サービスプロバイダ310に送信する。サービスプロバイダ310は、マーケティング情報データ904を参考にして、今後提供するサービスの内容を決定する。

【0345】以下、EMDサービスセンタ302内での処理の流れを説明する。EMDサービスセンタ302からSAM3051〜3054への配信用鍵データKD1〜KD3の送信は、第1実施形態の場合と同様に行なわれる。

【0346】また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開鍵証明書データの発行要求を受けた場合の処理は証明書・権利書管理部445が証明書データベース445bにアクセスする点を除いて、前述した第1実施形態と同じである。また、権利書データ106などを登録する処理も、証明書・権利書管理部445が権利書データベース445aに当該データを格納する点を除いて前述した第1実施形態の場合と同様である。

【0347】次に、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図70を参照しながら説明する。この場合に、サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子SPID、公開鍵データKsp、rおよび署名データSIGo、spをサービスプロバイダ310から受信すると、これらを、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データKessを用いて復号する。そして、当該復号した署名データSIGo、spの正当性を署名処理部443において確認した後に、識別子SPIDおよび公開鍵データKsp、rに基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。そして、証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データCERsを証明書データベース445bから読み出してサービスプロバイダ管理部390に出力する。また、署名処理部443は、公開鍵証明書データCERsのハッシュ値をとり、EMDサービスセンタ302の秘密鍵データKescを用いて、署名データSIGo、escを作成し、これをサービスプロバイダ管理部390に出力する。そして、サービスプロバイダ管理部390は、公開鍵証明書データCERs、rおよびその署名データSI

135

G01、ESCを、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0348】なお、EMDサービスセンタ302がSAM1051～1054から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106およびコンテンツ鍵データK_Cの登録要求を受けた場合の処理も、第1実施形態と同様である。また、EMDサービスセンタ302が、コンテンツプロバイダ301から受信した登録用モジュールMod₂に応じてキーファイルKFを作成してコンテンツプロバイダ301に送信する処理も、第1実施形態と同様である。

【0349】次に、EMDサービスセンタ302が、サービスプロバイダ310からブライスタグデータ312の登録要求を受けた場合の処理を、図70を参照しながら説明する。この場合には、サービスプロバイダ管理部390がサービスプロバイダ310から図69に示すブライスタグ登録要求モジュールMod₁₀₂を受信すると、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いてブライスタグ登録要求モジュールMod₁₀₂を復号する。そして、当該復号したブライスタグ登録要求モジュールMod₁₀₂に格納された署名データSIG₀₅、SRの正当性を署名処理部443において確認した後に、ブライスタグ登録要求モジュールMod₁₀₂に格納されたブライスタグデータ312を、証明書・権利書管理部445を介して権利書データベース445に登録して権威化する。

【0350】次に、EMDサービスセンタ302において決済を行なう場合の処理を図72を参照しながら説明する。SAM管理部149は、ユーザホームネットワーク303の例えばSAM3051から利用履歴データ308およびその署名データSIG₂₀₅、SAM₁を入力すると、利用履歴データ308および署名データSIG₂₀₅、SAM₁を、相互認証部150とSAM3051～3054と間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM3051の公開鍵データK_{SAM1P}を用いて署名データSIG₂₀₅、SAM₁の検証を行なった後に、決算処理部442に出力する。

【0351】そして、決算処理部442は、SAM3051から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびブライスタグデータ312とに基づいて決済処理を行う。決算処理部442は、決済処理により、図72に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ

136

152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決済機関管理部144に出力する。また、決済処理により、図70および図72に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決済機関管理部144に出力する。

【0352】次に、決算機関管理部144は、決済請求権データ152c、152sと、それらについて秘密鍵データK_{ESC}を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図59に示すペイメントゲートウェイ90を介して決済機関91に送信する。これにより、決済請求権データ152cに示される全額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される全額の金銭がサービスプロバイダ310に支払われる。

【0353】次に、EMDサービスセンタ302がコンテンツプロバイダ301およびサービスプロバイダ310に決済レポートデータ307cおよび307sを送信する場合の処理を説明する。決算処理部442において決済が行なわれると、決算処理部442からコンテンツプロバイダ管理部148に決済レポートデータ307cが出力される。コンテンツプロバイダ管理部148は、決算処理部442から決済レポートデータ307cを入力すると、これを、相互認証部150と図63に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ301に送信する。また、決算処理部442において決済が行なわれると、決算処理部442からサービスプロバイダ管理部390に決済レポートデータ307sが出力される。サービスプロバイダ管理部390は、決算処理部442から決済レポートデータ307sを入力すると、これを、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0354】EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM3051～3054の出荷時の処理と、SAM登録リストの登録処理とを行なう。

【0355】【ユーザホームネットワーク303】ユーザホームネットワーク303は、図59に示すように、ネットワーク機器360iおよびA/V機器360j～360nを有している。ネットワーク機器360iは、CAMジュール311およびSAM3051を内蔵している。また、AV機器360j～360nは、それぞれSAM3052～3054を内蔵している。SAM3051～3054の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続され

ている。なお、AV機器3602~3604は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器3601のネットワーク通信機能を利用してよい。また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0356】以下、ネットワーク機器3601について説明する。図74は、ネットワーク機器3601の構成図である。図74に示すように、ネットワーク機器3601は、通信モジュール162、CAモジュール311、復号モジュール905、SAM3051、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。図74において、図25と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

【0357】通信モジュール162は、サービスプロバイダ310との間の通信処理を行う。具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテンツ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310から電話回線などを介して受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0358】図75は、CAモジュール311および復号モジュール905の機能ブロック図である。図75に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データKses生成し、これを暗号化・復号部908に出力する。

【0359】記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データKmを記憶する。

【0360】暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データKscrおよびワーク鍵データKwを入力し、記憶部907から読み出したマスタ鍵データKmを用いてワーク鍵データKwを復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データKwを用いてスクランブル鍵データKscrを復号し、当該復号したスクランブル鍵データKscrを復号部910

に出力する。また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データKsesを用いて復号して復号モジュール905のセキュアコンテンツ選択部911に出力する。また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データKsesを用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

【0361】SP用購入履歴データ生成部909は、図74に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータCの購入操作に応じた操作信号S165、またはSAM3051からの利用制限状態データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履歴データ309を生成し、これを暗号化・復号部908に出力する。SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0362】なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0363】復号モジュール905は、復号部910およびセキュアコンテンツ選択部911を有する。復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテンツ304、スクランブル鍵データKscrおよびワーク鍵データKwを入力する。そして、復号部910は、暗号化されたスクランブル鍵データKscrおよびワーク鍵データKwをCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データKscrを入力する。そして、復号部910は、暗号化されたセキュアコンテンツ304を、スクランブル鍵データKscrを用いて復号した後に、セキュアコンテンツ選択部911に出力する。

【0364】なお、セキュアコンテンツ304が、MPEG2 Transport Stream方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet内のECM（Entitlement Control Message）からスクランブル鍵データKscrを取り出し、EMM（Entitlement Management

ent Message) からワーク鍵データ Kw を取り出す。ECM には、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ECM は、その他に、ユーザ（視聴者）毎に異なる個別視聴契約情報などが含まれている。

【0365】セキュアコンテナ選択部 911 は、復号部 910 から入力したセキュアコンテナ 304 を、CA ナビゲーション 311 から入力したユーザ嗜好フィルタデータ 900 を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ 304 を選択して SAM 305 1 に出力する。

【0366】次に、SAM 305 1 について説明する。なお、SAM 305 1 は、サービスプロバイダ 310 についての署名検証処理を行なうなど、コンテンツプロバイダ 301 に加えてサービスプロバイダ 310 に関しての処理を行う点を除いて、図 26 ～ 図 41 を用いて前述した第 1 実施形態の SAM 105 1 と基本的に同様な機能および構造を有している。また、SAM 305 1 は、SAM 305 1 と基本的に同じ機能を有している。すなわち、SAM 305 1 は、コンテンツ単位の課金処理をおこなうモジュールであり、EMD サービスセンタ 302 との間で通信を行う。

【0367】以下、SAM 305 1 の機能について詳細に説明する。図 76 は、SAM 305 1 の機能の構成図である。なお、図 76 には、サービスプロバイダ 310 からセキュアコンテナ 304 を入力する際の処理に関連するデータの流れが示されている。図 76 に示すように、SAM 305 1 は、相互認証部 170、暗号化・復号部 171、172、173、誤り訂正部 181、ダウンロードメモリ管理部 182、セキュアコンテナ復号部 183、復号・伸長モジュール管理部 184、EMD サービスセンタ管理部 185、利用監視部 186、署名処理部 189、SAM 管理部 190、記憶部 192、メディア SAM 管理部 197、スタックメモリ 200、サービスプロバイダ管理部 580、課金処理部 587、署名処理部 598 および外部メモリ管理部 811 を有する。なお、図 76 に示す SAM 305 1 の所定の機能は、SAM 105 1 の場合と同様に、CPU において秘密プログラムを実行することによって実現される。図 76 において、図 26 と同じ符号を付した機能ブロックは、第 1 実施形態で説明した同一符号の機能ブロックと同じである。

【0368】また、図 74 に示す外部メモリ 201 には、第 1 実施形態で説明した処理および後述する処理を経て、利用履歴データ 308 および SAM 登録リストが記憶される。また、スタックメモリ 200 には、図 77 に示すように、コンテンツ鍵データ Kc、権利書データ (UCP) 106、記憶部 192 のロック鍵データ KLoc、コンテンツプロバイダ 301 の公開鍵証明書データ CERcp、サービスプロバイダ 310 の公開鍵証

明書データ CERsp、利用制御状態データ (UCS) 366、SAM プログラム・ダウンロード・コンテナ SDCl ～ SDCh およびプライスタグデータ 312 などが記憶される。

【0369】以下、SAM 305 1 の機能ブロックのうち、図 76 において新たに符号を付した機能ブロックについて説明する。署名処理部 589 は、記憶部 192 あるいはスタックメモリ 200 から読み出した EMD サービスセンタ 302 の公開鍵データ KEscp、コンテンツプロバイダ 301 の公開鍵データ Kcp およびサービスプロバイダ 310 の公開鍵データ Ksp を用いて、セキュアコンテナ 304 内の署名データの検証を行なう。

【0370】課金処理部 587 は、図 78 に示すように、図 74 に示す購入・利用形態決定操作部 165 からの操作信号 S165 と、スタックメモリ 200 から読み出されたプライスタグデータ 312 とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。課金処理部 587 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御状態データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0371】また、課金処理部 587 は、課金処理において、利用履歴データ 308 を生成し、これを外部メモリ管理部 811 を介して外部メモリ 201 に書き込む。ここで、利用履歴データ 308 は、第 1 実施形態の利用履歴データ 108 と同様に、EMD サービスセンタ 302 において、セキュアコンテナ 304 に関連したライセンス料の支払いを決定する際に用いられる。

【0372】また、課金処理部 587 は、操作信号 S165 に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ 166 を生成し、これをスタックメモリ 200 に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 166 には、コンテンツの 1 D、購入形態、買い切り価格、当該コンテンツの購入が行なわれた SAM の SAM_ID、購入を行なったユーザの USER_ID などが記述されている。

【0373】なお、決定された購入形態が再生課金である場合には、例えば、SAM 305 1 からサービスプロバイダ 310 に利用制御状態データ 166 をリアルタイム

141

ムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ308をSAM1051に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制課状解除データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0374】また、SAM3051では、図76に示すように、EMDサービスセンタ管理部185を介してEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図74に示す復号モジュール905から入力したセキュアコンテナ304のうち、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM3051において、当該SAM3051のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0375】以下、SAM3051内での処理の流れを説明する。EMDサービスセンタ302から受信した配信鍵データKD1～KD3を記憶部192に格納する際のSAM3051内での処理の流れは、前述したSAM1051の場合と同様である。

【0376】次に、セキュアコンテナ304をサービスプロバイダ310から入力する際のSAM3051内での処理の流れを図76を参照しながら説明する。相互認証部170と図63に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。暗号化・復号部171は、当該相互認証によって得られたセッション鍵データKsesを用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図65に示すセキュアコンテナ304を復号する。

【0377】次に、署名処理部589は、図65(D)に示す署名データSIG1、ESC、SIG1、ESCの検証を行った後に、公開鍵証明書データCERSP、CERP内に格納された公開鍵データKSP、P、KCP、Pを用いて、署名データSIG6、CP、SIG62、SP、SIG7、CP、SIG63、SP、SIG64、SPの正当性を検証する。ここで、署名データSIG6、CP、SIG62、SPを検証することでコンテンツファイルCFの作成者および送信者の正当性が確認され、署名データSIG7、CP、SIG63、SPを検証することでキーファイルKFの送信者の正当性が確認され、署名データSIG

142

G64、SPを検証することでブライスタグデータ312の作成者および送信者の正当性が確認される。また、署名処理部589は、記憶部192から読み出した公開鍵データKESC、Pを用いて、図65(B)に示すキーファイルKFに格納された署名データSIGK1、ESCの正当性を検証することで、キーファイルKFの作成者の正当性、並びにキーファイルKFがEMDサービスセンタ302で登録されているか否かを検証する。

【0378】サービスプロバイダ管理部580は、署名処理部589において上述した全ての署名データの正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

【0379】誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。ダウンロードメモリ管理部182は、相互認証部170と図74に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

【0380】次に、ダウンロードメモリ管理部182は、相互認証部170と図74に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図65(B)に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0381】そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信鍵データKD1～KD3を用いて、図65(B)に示すキーファイルKFに格納されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1～SDC3が復号される。そして、復号されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1～SDC3がスタックメモリ200に書き込まれる。

【0382】以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図78および図79を参照しながら説明する。図79は、セキュアコンテナ304の購入形態決定処理を説明するためのフローチャートである。

＜ステップE1＞ユーザによる図74に示す購入・利用形態決定操作部165の操作によって、試験モードを示す操作信号S165が課金処理部587に出力された場合には、ステップE2の処理が行われ、そうでない場合にはステップE3の処理が行われる。

【0383】＜ステップE2＞試験モードを示す操作信号S165が課金処理部587に出力された場合に行われ、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管

143

理部 184 を介して、図 74 に示す復号・伸長モジュール 163 に出力される。このとき、コンテンツファイル CF に対して、相互認証部 170 とメディア SAM167a との間の相互認証およびセッション鍵データ KSES による暗号化・復号と、相互認証部 170 と相互認証部 220 との間の相互認証およびセッション鍵データ KSES による暗号化・復号とが行なわれる。コンテンツファイル CF は、図 74 に示す復号部 221 においてセッション鍵データ KSES を用いて復号された後に、復号部 222 に出力される。

【0384】また、スタックメモリ 200 から読み出されたコンテンツ鍵データ Kc および半開示パラメータデータ 199 が、図 74 に示す復号・伸長モジュール 163 に出力される。このとき、相互認証部 170 と相互認証部 220 との間の相互認証後に、コンテンツ鍵データ Kc および半開示パラメータデータ 199 に対してセッション鍵データ KSES による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ 199 が半開示処理部 225 に出力され、半開示処理部 225 からの制御によって、復号部 222 によるコンテンツ鍵データ Kc を用いたコンテンツデータ C の復号が半開示で行われる。次に、半開示で復号されたコンテンツデータ C が、伸長部 223 において伸長された後に、電子透かし情報処理部 224 に出力される。次に、電子透かし情報処理部 224 においてユーザ電子透かし情報用データ 196 がコンテンツデータ C に埋め込まれた後、コンテンツデータ C が再生モジュール 169 において再生され、コンテンツデータ C に応じた音響が出力される。

【0385】<ステップ E3> ユーザが、購入・利用形態決定操作部 165 を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S165 が購入処理部 187 に出力される。

【0386】<ステップ E4> 課金処理部 187 において、決定された購入形態に応じた利用履歴データ 308 および利用制御状態データ 166 が生成され、利用履歴データ 308 が外部メモリ管理部 811 を介して外部メモリ 201 に書き込まれると共に利用制御状態データ 166 がスタックメモリ 200 に書き込まれる。以後は、利用監視部 186 において、利用制御状態データ 166 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ 200 に格納されているキーファイル KF と、利用制御状態データ 166 とを用いて、購入形態が決定した後述する図 81 (C) に示す新たなキーファイル KF₁ が生成され、当該作成されたキーファイル KF₁ がスタックメモリ 200 に記憶される。図 81

(C) に示すように、キーファイル KF₁ に格納された利用制御状態データ 166 はストレージ鍵データ KSTR およびメディア鍵データ KMED を用いて DES の CBC モードを利用して順に暗号化されている。こ

144

で、記録用鍵データ KSTR は、例えば SACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R 機器および MD (Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。また、メディア鍵データ KMED は、記録媒体にユニークなデータである。

【0387】また、署名処理部 589 において、SAM305₁ の秘密鍵データ K_{SAM1} を用いて、キーファイル KF₁ のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル KF₁ に対応付けられて、スタックメモリ 200 に記憶される。

【0388】<ステップ E5> SAM305₁ から EMD サービスセンタ 302 に、利用制御状態データ 166 が送信される。当該利用制御状態データ 166 の送信は、SAM305 において、コンテンツデータの購入形態が決定される度に行われる。なお、SAM305₁ から EMD サービスセンタ 302 への利用履歴データ 308 の送信は、例えば、例えば、1 個月などの所定の時間間隔で行われる。

【0389】次に、ダウンロードメモリ 167 に記憶されている購入形態が既に決定されたコンテンツデータ C を再生する場合の処理の流れを、図 78 を参照しながら説明する。この場合には、利用監視部 186 の監視下で、操作信号 S165 に基づいて、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、図 74 に示す復号・伸長モジュール 163 に出力される。

また、スタックメモリ 200 から読み出されたコンテンツ鍵データ Kc が復号・伸長モジュール 163 に出力される。そして、復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ Kc を用いたコンテンツファイル CF の復号と、伸長部 223 による伸長処理とが行なわれ、再生モジュール 169 において、コンテンツデータ C が再生される。このとき、課金処理部 587 において、操作信号 S165 に応じて、外部メモリ 201 に記憶されている利用履歴データ 308 が更新される。利用履歴データ 308 は、秘密鍵データ K_{SAM1} を用いて作成した署名データ SIG205₁、SAM と共に、EMD サービスセンタ管理部 186 を介して、所定のタイミングで、EMD サービスセンタ 302 に送信される。

【0390】次に、図 80 に示すように、例えば、ネットワーク機器 360₁ のダウンロードメモリ 167 にダウンロードされた既に購入形態が決定された図 81 に示すセキュアコンテンツ 304 を、バス 191 を介して、AV 機器 360₂ の SAM305₂ に転送する場合の SAM305₁ ユーザでの処理の流れを図 82 を参照しながら説明する。内では、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所

定のコンテンツをAV機器3602に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部587に出力される。これにより、課金処理部587は、操作信号S165に基づいて、スタックメモリ200に記憶されている利用履歴データ308を更新する。

【0391】また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図81

(A)、(B)、(C)に示すコンテンツファイルCFおよびキーファイルKF、KF1を署名処理部589およびSAM管理部190に出力する。そして、署名処理

部589は、コンテンツファイルCFおよびキーファイルKFの署名データSIG41、SAM1、SIG

42、SAM1を作成すると共に、キーファイルKF1のハッシュ値HK1を作成し、これらをSAM管理部190に出力する。また、SAM管理部190は、図81

(D)、(E)に示すブライスタグデータ312およびその署名データSIG64、SPと、公開鍵証明書データCERCPおよびその署名データSIG1、ESCとをスタックメモリ200から読み出す。また、SAM管理

部190は、図81(E)に示す公開鍵証明書データCERSAM1およびその署名データSIG

22、ESCを記憶部192から読み出す。

【0392】次に、SAM管理部190は、図81に示すセキュアコンテンツ304xを作成する。また、相互認証部170は、SAM3052との間で相互認証を行って得たセッション鍵データKSESを暗号化・復号部171に出力する。SAM管理部190は、図81に示す

セキュアコンテンツ304xを、暗号化・復号部171において、セッション鍵データKSESを用いて暗号化した後に、図82に示すAV機器3602のSAM305

2に出力する。

【0393】以下、図80に示すように、SAM3051から入力したセキュアコンテンツ304xを、RAM型

な記録媒体(メディア)に書き込む際のSAM3052内での処理の流れを、図83を参照しながら説明する。

【0394】この場合には、SAM3052のSAM管理部190は、図83に示すように、図81に示すセキュアコンテンツ304xを、ネットワーク機器3601のSAM3051から入力する。そして、SAM3051の相互認証部170とSAM3052の相互認証部170との間の相互認証が行われ、署名処理部589において、当該相互認証によって得られたセッション鍵データKSESを用いて、セキュアコンテンツ304xの復号が行われる。次に、署名処理部589において、記憶部192から読み出した公開鍵データKRC、Pを用いて、図81(E)に示す署名データSIG61、ESC、SIG1、ESC、SIG22、ESCの正当性を検証する。そして、署名データSIG61、ESC、SIG

1、ESC、SIG22、ESCの正当性が確認される

と、署名処理部589において、公開鍵証明書データCERCP、CERCP、CERSAM1に含まれる公開鍵データKSP、P、KCP、P、KSP、Pを用いて、図81(A)～(D)に示す署名データSIG

a、CP、SIG62、SP、SIG41、SAM1、SIG7、CP、SIG63、SP、SIG

42、SAM1、SIG64、SPおよびハッシュ値HK1の正当性が検証される。そして、これらの署名データの正当性が確認されたら、スタックメモリ200に、キーファイルKF、KF1およびブライスタグデータ312が記憶される。また、コンテンツファイルCFが、SAM管理部190から記録モジュール管理

部855に出力される。そして、図81(C)に示すキーファイルKF1に格納されたコンテンツ鍵データKcおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMedおよび購入者鍵データKPINを用いて順に暗号化された後に記録モジュール管理

部855に出力される。また、スタックメモリ200から読み出されたキーファイルKFが、記録モジュール管理

部855に出力される。そして、相互認証部170とRAM型の記録媒体1304のメディアSAM133との間の相互認証を行った後に、コンテンツファイルCFがRAM型の記録媒体1304のセキュアでないRAM領域134に記憶され、キーファイルKF、KF1およびブライスタグデータ312がセキュアRAM領域132に書き込まれる。なお、キーファイルKF、KF1およびブライスタグデータ312を、RAM型の記録媒体1304のメディアSAM133に記憶する

ようにしてもよい。

【0395】なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のRAM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器3602において購入形態が未決定のROM型の記録媒体からセキュアコンテンツ304xを読み出してこれをAV機器3602に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にブライスタグデータ312を格納する点を除いて、第1実施形態のSAM1051の場合と同じである。

【0396】次に、図59に示すEMDシステム300の全体動作について説明する。図84および図85は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を示して説明する。なお、以下に示す処理の前提として、EMDサービスシステム302へのコンテンツプロバイダ301、サービスプロバイ

と、署名処理部589において、公開鍵証明書データCERCP、CERCP、CERSAM1に含まれる公開鍵データKSP、P、KCP、P、KSP、Pを用いて、図81(A)～(D)に示す署名データSIG

a、CP、SIG62、SP、SIG41、SAM1、SIG7、CP、SIG63、SP、SIG

42、SAM1、SIG64、SPおよびハッシュ値HK1の正当性が検証される。そして、これらの署名データの正当性が確認されたら、スタックメモリ200に、キーファイルKF、KF1およびブライスタグデータ312が記憶される。また、コンテンツファイルCFが、SAM管理部190から記録モジュール管理

部855に出力される。そして、図81(C)に示すキーファイルKF1に格納されたコンテンツ鍵データKcおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMedおよび購入者鍵データKPINを用いて順に暗号化された後に記録モジュール管理

部855に出力される。また、スタックメモリ200から読み出されたキーファイルKFが、記録モジュール管理

部855に出力される。そして、相互認証部170とRAM型の記録媒体1304のメディアSAM133との間の相互認証を行った後に、コンテンツファイルCFがRAM型の記録媒体1304のセキュアでないRAM領域134に記憶され、キーファイルKF、KF1およびブライスタグデータ312がセキュアRAM領域132に書き込まれる。なお、キーファイルKF、KF1およびブライスタグデータ312を、RAM型の記録媒体1304のメディアSAM133に記憶する

ようにしてもよい。

【0395】なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器3602において購入形態が未決定のROM型の記録媒体からセキュアコンテンツ304xを読み出してこれをAV機器3602に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にブライスタグデータ312を格納する点を除いて、第1実施形態のSAM1051の場合と同じである。

【0396】次に、図59に示すEMDシステム300の全体動作について説明する。図84および図85は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を示して説明する。なお、以下に示す処理の前提として、EMDサービスシステム302へのコンテンツプロバイダ301、サービスプロバイ

と、署名処理部589において、公開鍵証明書データCERCP、CERCP、CERSAM1に含まれる公開鍵データKSP、P、KCP、P、KSP、Pを用いて、図81(A)～(D)に示す署名データSIG

a、CP、SIG62、SP、SIG41、SAM1、SIG7、CP、SIG63、SP、SIG

42、SAM1、SIG64、SPおよびハッシュ値HK1の正当性が検証される。そして、これらの署名データの正当性が確認されたら、スタックメモリ200に、キーファイルKF、KF1およびブライスタグデータ312が記憶される。また、コンテンツファイルCFが、SAM管理部190から記録モジュール管理

部855に出力される。そして、図81(C)に示すキーファイルKF1に格納されたコンテンツ鍵データKcおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMedおよび購入者鍵データKPINを用いて順に暗号化された後に記録モジュール管理

部855に出力される。また、スタックメモリ200から読み出されたキーファイルKFが、記録モジュール管理

部855に出力される。そして、相互認証部170とRAM型の記録媒体1304のメディアSAM133との間の相互認証を行った後に、コンテンツファイルCFがRAM型の記録媒体1304のセキュアでないRAM領域134に記憶され、キーファイルKF、KF1およびブライスタグデータ312がセキュアRAM領域132に書き込まれる。なお、キーファイルKF、KF1およびブライスタグデータ312を、RAM型の記録媒体1304のメディアSAM133に記憶する

ようにしてもよい。

【0395】なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器3602において購入形態が未決定のROM型の記録媒体からセキュアコンテンツ304xを読み出してこれをAV機器3602に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にブライスタグデータ312を格納する点を除いて、第1実施形態のSAM1051の場合と同じである。

【0396】次に、図59に示すEMDシステム300の全体動作について説明する。図84および図85は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を示して説明する。なお、以下に示す処理の前提として、EMDサービスシステム302へのコンテンツプロバイダ301、サービスプロバイ

と、署名処理部589において、公開鍵証明書データCERCP、CERCP、CERSAM1に含まれる公開鍵データKSP、P、KCP、P、KSP、Pを用いて、図81(A)～(D)に示す署名データSIG

a、CP、SIG62、SP、SIG41、SAM1、SIG7、CP、SIG63、SP、SIG

42、SAM1、SIG64、SPおよびハッシュ値HK1の正当性が検証される。そして、これらの署名データの正当性が確認されたら、スタックメモリ200に、キーファイルKF、KF1およびブライスタグデータ312が記憶される。また、コンテンツファイルCFが、SAM管理部190から記録モジュール管理

部855に出力される。そして、図81(C)に示すキーファイルKF1に格納されたコンテンツ鍵データKcおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMedおよび購入者鍵データKPINを用いて順に暗号化された後に記録モジュール管理

部855に出力される。また、スタックメモリ200から読み出されたキーファイルKFが、記録モジュール管理

部855に出力される。そして、相互認証部170とRAM型の記録媒体1304のメディアSAM133との間の相互認証を行った後に、コンテンツファイルCFがRAM型の記録媒体1304のセキュアでないRAM領域134に記憶され、キーファイルKF、KF1およびブライスタグデータ312がセキュアRAM領域132に書き込まれる。なお、キーファイルKF、KF1およびブライスタグデータ312を、RAM型の記録媒体1304のメディアSAM133に記憶する

ようにしてもよい。

【0395】なお、SAM3051内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器3602内での処理の流れ、AV機器3602において購入形態が未決定のROM型の記録媒体からセキュアコンテンツ304xを読み出してこれをAV機器3602に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にブライスタグデータ312を格納する点を除いて、第1実施形態のSAM1051の場合と同じである。

【0396】次に、図59に示すEMDシステム300の全体動作について説明する。図84および図85は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を示して説明する。なお、以下に示す処理の前提として、EMDサービスシステム302へのコンテンツプロバイダ301、サービスプロバイ

ダ310およびSAM3051~3054の登録は既に終了しているものとする。

【0397】ステップS21：EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKCP、Pの公開鍵証明書CERCPを、自らの署名データSIG1、ESCと共にコンテンツプロバイダ301に送信する。また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データKSP、Pの公開鍵証明書CERSPを、自らの署名データSIG61、ESCと共にサービスプロバイダ310に送信する。また、EMDサービスセンタ302は、各々有効期限が1カ月の3カ月分の配信用鍵データKD1~KD3をユーザホームネットワーク303のSAM3051~3054に送信する。

【0398】ステップS22：コンテンツプロバイダ301は、相互認証を行った後に、図18に示す登録用モジュールModuleを、EMDサービスセンタ302に送信する。そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。また、EMDサービスセンタ302は、登録用モジュールModuleに応じた図5(B)に示す6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ301に送信する。

【0399】ステップS23：コンテンツプロバイダ301は、図5(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG6、CPTと、キーファイルKFおよびその署名データSIG7、CPTを作成し、これらと図5(C)に示す公開鍵証明書データCERCPおよびその署名データSIG1、ESCとを格納したセキュアコンテンツ104を、オンラインおよび/またはオフラインで、サービスプロバイダ310に提供する。

【0400】ステップS24：サービスプロバイダ310は、図5(C)に示す署名データSIG1、ESCを検証した後に、公開鍵証明書データCERCPに格納された公開鍵データKCP、Pを用いて、図5(A)、(B)に示す署名データSIG6、CPTおよびSIG7、CPTを検証して、セキュアコンテンツ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0401】ステップS25：サービスプロバイダ310は、ブライスタグデータ312およびその署名データSIG64、SPを作成し、これらを格納した格納した図65に示すセキュアコンテンツ304を作成する。

【0402】ステップS26：サービスプロバイダ310は、図65に示すブライスタグ登録要求モジュールModuleを、EMDサービスセンタ302に送信する。そして、EMDサービスセンタ302は、所定の署名検証を行った後に、ブライスタグデータ312を登録

して権威化する。

【0403】ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAMモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテンツ304を、オンラインあるいはオフラインで、図74に示すネットワーク機器3601の復号モジュール905に送信する。

【0404】ステップS28：CAMモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0405】ステップS29：SAM3051~3054のいずれかにおいて、図65(D)に示す署名データSIG61、ESCを検証した後に、公開鍵証明書データCERSPに格納された公開鍵データKSP、Pを用いて、図65(A)、(B)、(C)に示す署名データSIG62、SP、SIG63、SP、SIG64、SPを検証して、セキュアコンテンツ304内の所定のデータが正当なサービスプロバイダ310において作成および送信されたか否かを確認する。

【0406】ステップS30：SAM3051~3054のいずれかにおいて、図65(D)に示す署名データSIG1、ESCを検証した後に、公開鍵証明書データCERCPに格納された公開鍵データKCP、Pを用いて、図65(A)、(B)、(C)に示す署名データSIG6、SP、SIG7、SPを検証して、セキュアコンテンツ304内のコンテンツファイルCFが正当なコンテンツプロバイダ301において作成されたか否かと、キーファイルKFが正当なコンテンツプロバイダ301から送信されたか否かを確認する。また、SAM3051~3054のいずれかにおいて、公開鍵データKESC、Pを用いて、図65(B)に示すキーファイルKF内の署名データSIG61、ESCの正当性を検証することで、キーファイルKFが正当なEMDサービスセンタ302によって作成されたか否かを確認する。

【0407】ステップS31：ユーザが図74の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

【0408】ステップS32：ステップS31において生成された操作信号S165に基づいて、SAM3051~3054において、セキュアコンテンツ304の利用履歴(Usage Log)データ308が生成される。SAM3051~3054からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG208、SAMIが送信される。また、購入形態が決定される度にリアルタイムに、SAM3051~3054からEMDサービスセンタ302に利用制御状態データ166が送信される。

【0409】ステップS33：EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテン

149

プロバイダ301およびサービスプロバイダ310の各々について、課金内容(計算)し、その結果に基づいて、決済請求権データ152c、152sを作成する。

【0410】ステップS34: EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0411】以上説明したように、EMDシステム300では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305へ305a内で行う。また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD1〜KD3を用いて暗号化されており、配信鍵データKD1〜KD3を保持しているSAM305a〜305d内でのみ復号される。そして、SAM305a〜305dでは、附随性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

【0412】従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300によれば、権利書データ106をサービスプロバイダ310が管理できないよう系列。そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303における当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0413】また、EMDシステム300では、セキュアコンテナ104、304内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ310およびSAM305a〜305dにおいて、それらの作成者および送信者の正当性、並びにそれらが改竄されていないかなどを確認できる。その結果、コ

150

ンテンツデータCの不正利用を効果的に回避できる。

【0414】また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305a〜305dにおけるコンテンツデータCの権利処理を共通化できる。

【0415】また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器360aおよびAV機器360s〜360dにおいてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。例えば、図86に示すように、コンテンツプロバイダ301が提供したコンテンツデータCを、サービスプロバイダ310からユーザホームネットワーク303に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法(経路)で配信(配給)した場合でも、ユーザホームネットワーク303、303aのSAMにおいて、コンテンツプロバイダ301が作成した権利書データ106に基づいて、共通の権利処理ルールが採用される。

【0416】また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305a〜305dに供給される。従って、SAM305a〜305dにおいて、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0417】以下、上述した第2実施形態のEMDシステム300で採用するセキュアコンテナなどの配送プロトコルの具体例について説明する。図87に示すように、コンテンツプロバイダ301において作成されたセキュアコンテナ104は、インターネット(TCP/IP)あるいは専用線(ATMCell)などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバ

151

イダ310に提供される。また、サービスプロバイダ310は、セキュアコンテナ104を用いて作成したセキュアコンテナ304を、デジタル放送(MPEG-TS)のXML/SMIL)、インターネット(TCP/IP)上のXML/SMIL)あるいはパッケージ流通(記録媒体)などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク303に配給する。また、ユーザホームネットワーク303、303a内、あるいはユーザホームネットワーク303と303aとの間において、SAM相互間で、セキュアコンテナが、家庭内EC/配信サービス(1394シリアルバス・インターフェイス上のXML/SMIL)や記録媒体などを用いて転送される。

【0418】以下、図87において、符号A~Gを用いた経路におけるデータ転送に採用される配送プロトコルの一例を詳細に説明する。図88は、図87に示すコンテンツプロバイダ301とサービスプロバイダ310との間(符号A)でセキュアコンテナ104などを転送するとき採用される配送プロトコルを説明するための図である。図88に示すように、コンテンツプロバイダ301からサービスプロバイダ310にセキュアコンテナ104などが、IP/IP-SEC層、SSL(Secure Sockets Layer)層、XML(Extensible Markup Language)/SMIL(Synchronized Multimedia Integration Language)層およびアプリケーション層において共通鍵を用いたセッションを行って転送される。

【0419】図89は、図87に示すEMDサービスセンタ302とコンテンツプロバイダ301との間(符号H)でキープファイルなどを転送するときに採用される配送プロトコルを説明するための図である。図89に示すように、EMDサービスセンタ302からコンテンツプロバイダ301にキープファイルなどが、IP/IP-SEC層、SSL層およびアプリケーション層において共通鍵を用いたセッションを行って転送される。

【0420】図90は、図に示すEMDサービスセンタ302とサービスプロバイダ310との間(符号C)でブライスタグデータ312などを転送するときに採用される配送プロトコルを説明するための図である。図90に示すように、EMDサービスセンタ302からサービスプロバイダ310にブライスタグデータ312などが、IP/IP-SEC層、SSL層およびアプリケーション層において共通鍵を用いたセッションを行って転送される。

【0421】図91は、図87に示すサービスプロバイダ310とユーザホームネットワーク303との間(符号D)、ユーザホームネットワーク303内(符号E)で、セキュアコンテナ304などを転送するときに採用される配送プロトコルを説明するための図である。図9

152

1に示すように、サービスプロバイダ310からユーザホームネットワーク303のネットワーク機器360:1にセキュアコンテナ304などが転送される。このとき、サービスプロバイダ310とネットワーク機器360:1との間では、MPEG-TS層、PES層またはDSM_CC_Data_Carousel層、および、MHEG(Multimedia and Hypermedia Experts)層または「http層およびXML/SMIL層」が、セキュアコンテナ304を転送するためのサービスプロバイダ用商品配送プロトコルとして用いられる。また、ネットワーク機器360:1とストレージ機器360:2との間、並びにAV機器相互間では、HAVI(XMFL)が、セキュアコンテナを転送するためのユーザホームネットワーク商品配送プロトコルとして用いられる。このとき、デジタル放送のデータ放送方式にXML/SMIL/BMLを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキープファイルKF1、KF2と視聴(デモ)サンプルは、図92に示すようにHTTP層上のHML/XMFL/SMIL層およびモノメディアデータ層に格納されて転送される。また、デジタル放送のデータ放送方式にMHEGを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキープファイルKF1、KF2と視聴(デモ)サンプルは、図93に示すようにMHEG層上のモノメディアデータ層に格納されて転送される。また、デジタル放送のデータ放送方式にXML/SMILを利用した場合には、セキュアコンテナ304のコンテンツファイルCF1、CF2およびキープファイルKF1、KF2と視聴(デモ)サンプルは、図94に示すようにHTTP層上のXML/SMIL層に格納されて転送される。

【0422】図95は、図87に示すEMDサービスセンタ302とユーザホームネットワーク303、303aとの間(符号G)で、利用履歴データ308および利用制御状態データ166などを転送するときに採用される配送プロトコルを説明するための図である。図95に示すように、ネットワーク機器360:1からEMDサービスセンタ302に、利用履歴データ308などが転送される場合には、IP/IP-SEC層、SSL層およびアプリケーション層において、セッション鍵データを用いたセッションが行われる。また、ネットワーク機器360:2などがEMDサービスセンタ302に利用履歴データ308および利用制御状態データ166などを転送する場合には、利用履歴データ308などが、IP/IP-SEC層およびHAVI層でセッションを行ってストレージ機器360:2からネットワーク機器360:1に転送された後に、ネットワーク機器360:1からEMDサービスセンタ302に前述したように転送される。

【0423】図96は、図87に示すユーザホームネットワーク303のストレージ機器360:1からユーザホ

153

ームネットワーク303aのストレージ機器3601に、セキュアコンテナを配送するときに採用される配送プロトコルを説明するための図である。図96に示すように、ストレージ機器3604からストレージ機器3601にセキュアコンテナが、IP/1P-SEC層、SSL層、XML/SM1層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【0424】第2実施形態の第1変形例

図97は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。図97において、図59と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。図97に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

【0425】サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器3601に配給する。また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bとを格納したセキュアコンテナ304bを作成し、これをネットワーク機器3601に配給する。ここで、セキュアコンテナ304a、304bのフォーマットは、図65を用いた説明したセキュアコンテナ304と同じである。

【0426】ネットワーク機器3601には、サービスプロバイダ310a、310bの各々に対応したCAモジュール311a、311bが設けられている。CAモジュール311a、311bは、自らの要求に応じたセキュアコンテナ304a、304bの配給を、それぞれサービスプロバイダ310a、310bから受ける。

【0427】次に、CAモジュール311a、311bは、配給されたセキュアコンテナ304a、304bに応じたSP用購入履歴データ309a、309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a、310bに送信する。また、CAモジュール311a、311bは、セキュアコンテナ304a、304bをセッション鍵データKsesで復号した後に、SAM3051~3054に出力する。

【0428】次に、SAM3051~3054において、共通の配信用鍵データKD1~KD3を用いて、セキュアコンテナ304a、304b内のキープファイルK

154

Fが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

【0429】そして、SAM3051~3054からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0430】EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ152c、152sa、152sbを作成する。

【0431】EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sa、152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの所有者に分配される。

【0432】上述したように、EMDシステム300aによれば、同じコンテンツファイルCFをサービスプロバイダに310a、310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD1~KDdで暗号化してサービスプロバイダに310a、310bに供給し、サービスプロバイダに310a、310bは暗号化された権利書データ106をそのまま格納したセキュアコンテナ304a、304bをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のSAM3051~3054では、コンテンツファイルCFをサービスプロバイダに310a、310bの何れから配給を受けた場合でも、共通の権利書データ106に基づいて権利処理を行うことができる。

【0433】なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【0434】第2実施形態の第2変形例

図98は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステム300bの構成図である。図98において、図59と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。図98に示すように、EMDシステム300bでは、EMDサービスセンタ302からコンテンツプロバイダ301a、301bにそれぞれキーファイルKF a、KF bが供給され、コンテンツプロバイダ301a、301bからサービスプロバイダ310に、それぞれセキュアコンテナ104a、104bが供給される。

【0435】サービスプロバイダ310は、例えば、コ

155

コンテンツプロバイダ 301a、301b が供給したコンテンツを用いてサービスを提供しており、セキュアコンテンツ 104a についてのプライスタグデータ 312a と、セキュアコンテンツ 104b についてのプライスタグデータ 312b とをそれぞれ生成し、これらを格納したセキュアコンテンツ 304c を作成する。図 98 に示すように、セキュアコンテンツ 304c には、コンテンツファイル Cfa、CFb、キーファイル KFa、KFb、プライスタグデータ 312a、312b、それらの各々についてのサービスプロバイダ 310 の秘密鍵データ Kc、s による署名データが格納されている。

【0436】セキュアコンテンツ 304c は、ユーザホームネットワーク 303 のネットワーク機器 360 の C/A モジュール 311 で受信された後に、SAM3051 ~ 3054 において処理される。

【0437】SAM3051 ~ 3054 では、配信用鍵データ KD a1 ~ KD a s を用いて、キーファイル KFa が復号され、権利書データ 106a に基づいて、コンテンツファイル Cfa についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。また、SAM3051 ~ 3054 において、配信用鍵データ KD b1 ~ KD b s を用いて、キーファイル KFb が復号され、権利書データ 106b に基づいて、コンテンツファイル Cfb についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

【0438】そして、SAM3051 ~ 3054 から EMD サービスセンタ 302 に、利用履歴データ 308 が送信される。

【0439】EMD サービスセンタ 302 では、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301a、301b およびサービスプロバイダ 310 の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152c a、152c b、152c s を作成する。

【0440】EMD サービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152c a、152c b、152c s を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301a、301b およびサービスプロバイダ 310 の所有者に分配される。

【0441】上述したように、EMD システム 300b によれば、セキュアコンテンツ 304c 内に格納されたコンテンツファイル Cfa、CFb の権利書データ 106a、106b は、コンテンツプロバイダ 301a、301b が作成したものをそのまま用いるため、SAM3051 ~ 3054 内において、権利書データ 106a、106b に基づいて、コンテンツファイル Cfa、CFb

156

についての権利処理がコンテンツプロバイダ 301a、301b の意向に沿って確実に行われる。

【0442】なお、図 98 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【0443】第 2 実施形態の第 3 変形例

図 99 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。上述した第 2 実施形態では、EMD サービスセンタ 302 が決済機関 91 に対して、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済を行う場合を例示したが、本発明では、例えば、図 99 に示すように、EMD サービスセンタ 302 において、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 のための決済請求権データ 152c と、サービスプロバイダ 310 のための決済請求権データ 152s とを作成し、これらをそれぞれコンテンツプロバイダ 301 およびサービスプロバイダ 310 に送信するようにしてもよい。この場合には、コンテンツプロバイダ 301 は、決済請求権データ 152c を用いて、ペイメントゲートウェイ 90 a を介して決済機関 91 a に決済を行う。また、サービスプロバイダ 310 は、決済請求権データ 152s を用いて、ペイメントゲートウェイ 90 b を介して決済機関 91 b に決済を行う。

【0444】第 2 実施形態の第 4 変形例

図 100 は、第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。上述した第 2 実施形態では、例えば現行のインターネットのようにサービスプロバイダ 310 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 310 が課金機能を有している場合には、C/A モジュール 311 において、セキュアコンテンツ 304 に関するサービスプロバイダ 310 のサービスに対しての利用履歴データ 308 s を作成してサービスプロバイダ 310 に送信する。そして、サービスプロバイダ 310 は、利用履歴データ 308 s に基づいて、課金処理を行って決済請求権データ 152s を作成し、これを用いてペイメントゲートウェイ 90 b を介して決済機関 91 b に決済を行う。一方、SAM3051 ~ 3054 は、セキュアコンテンツ 304 に関するコンテンツプロバイダ 301 の権利処理に対しての利用履歴データ 308 c を作成し、これを EMD サービスセンタ 302 に送信する。EMD サービスセンタ 302 は、利用履歴データ 308 c に基づいて、決済請求権データ 152c を作成し、これをコンテンツプロバイダ 301 に送信する。コンテンツプロバイダ 301 は、決済請求権データ 152c を用いて、ペイメントゲートウェイ 90 a を介して決済機関 91 a に決済を行う。

【0445】第 2 実施形態の第 5 変形例

上述した実施形態では、図72に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM305_iなどから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図78に示すSAM305_iなどの利用履歴部186で生成されてリアルタイムにEMDサービスセンタ302に送信された利用制御状態データ166に基づいて、ユーザ嗜好フィルタ生成部901においてユーザ嗜好フィルタデータ903を生成してもよい。

【0446】第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM305_i～305₄は、それぞれ自らの公開鍵データK_{CP, P}, K_{SP, P}, K_{SAM1, P}～K_{SAM4, P}の他に、自らの秘密鍵データK_{CP, S}, K_{SP, S}, K_{SAM1, S}～K_{SAM4, S}をEMDサービスセンタ302に登録してもよい。このようにすることで、EMDサービスセンタ302は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データK_{CP, S}, K_{SP, S}, K_{SAM1, S}～K_{SAM4, S}を用いて、コンテンツプロバイダ301とサービスプロバイダ310との間の通信、サービスプロバイダ310とSAM305_i～305₄との間の通信、並びにユーザホームネットワーク303内のSAM305_i～305₄相互間での通信のうち対象となる通信を盗聴することが可能になる。また、SAM305_i～305₄については、出荷時に、EMDサービスセンタ302によって秘密鍵データK_{SAM1, S}～K_{SAM4, S}を生成し、これをSAM305_i～305₄に格納すると共にEMDサービスセンタ302が保持（登録）するようにしてもよい。

【0447】第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305_i～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAM4}を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305_i～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAM4}を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305_i～305₄が、通信時に、EMDサービスセンタ302から公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAM4}

を取得してもよい。

【0448】図101は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。なお、図101において、図59と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM305_i～305₄を接続している。

【0449】コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データCER_{SP}を取得する場合には、例えば、通信に先立ってサービスプロバイダ310からコンテンツプロバイダ301に公開鍵証明書データCER_{SP}を送信する場合（図101中（3））と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データCER_{SP}を取り寄せる場合（図101中（1））とがある。

【0450】また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明書データCER_{CP}を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ301からサービスプロバイダ310に公開鍵証明書データCER_{CP}を送信する場合（図101中（2））と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCER_{CP}を取り寄せる場合（図101中（4））とがある。

【0451】また、サービスプロバイダ310がSAM305_i～305₄の公開鍵証明書データCER_{SAM1}～CER_{SAM4}を取得する場合には、例えば、通信に先立ってSAM305_i～305₄からサービスプロバイダ310に公開鍵証明書データCER_{SAM1}～CER_{SAM4}を送信する場合（図101中（6））と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データCER_{SAM1}～CER_{SAM4}を取り寄せる場合（図101中（4））とがある。

【0452】また、SAM305_i～305₄がサービスプロバイダ310の公開鍵証明書データCER_{SP}を取得する場合には、例えば、通信に先立ってサービスプロバイダ310からSAM305_i～305₄に公開鍵証明書データCER_{SP}を送信する場合（図101中（5））と、SAM305_i～305₄がEMDサービスセンタ302から公開鍵証明書データCER_{SP}を取り寄せる場合（図101中（7）など）とがある。

【0453】また、SAM305_iがSAM305_jの公開鍵証明書データCER_{SAM2}を取得する場合には、例えば、通信に先立ってSAM305_jからSAM305_iに公開鍵証明書データCER_{SAM2}を送信する場合（図101中（8））と、SAM305_iがEMDサービスセンタ302から公開鍵証明書データCER

159

SAM2を取り寄せる場合(図101中(7)など)とがある。

【0454】また、SAM3052がSAM3051の公開鍵証明書データCER_SAM1を取得する場合には、例えば、通信に先立ってSAM3051からSAM3052に公開鍵証明書データCER_SAM1を送信する場合(図101中(9))と、SAM3052が自らEMDサービスセンタ302から公開鍵証明書データCER_SAM1を取り寄せる場合と、SAM3051が搭載されたネットワーク機器を介して公開鍵証明書データCER_SAM1を取り寄せる場合(図101中(7)、(8))とがある。

【0455】また、SAM3054がSAM3053の公開鍵証明書データCER_SAM13を取得する場合には、例えば、通信に先立ってSAM3053からSAM3054に公開鍵証明書データCER_SAM13を送信する場合(図101中(12))と、SAM3054が自らEMDサービスセンタ302から公開鍵証明書データCER_SAM13を取り寄せる場合(図101中(10))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_SAM13を取り寄せる場合とがある。

【0456】また、SAM30513がSAM3054の公開鍵証明書データCER_SAM14を取得する場合には、例えば、通信に先立ってSAM3054からSAM30513に公開鍵証明書データCER_SAM14を送信する場合(図101中(11))と、SAM30513が自らEMDサービスセンタ302から公開鍵証明書データCER_SAM14を取り寄せる場合(図101中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_SAM14を取り寄せる場合とがある。

【0457】第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054に送信する。なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054において生成してもよい。

【0458】まず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCER

160

CPを無効にする場合について説明する。図102に示すように、EMDサービスセンタ302は、公開鍵証明書データCERCPを無効にすることを示す公開鍵証明書破棄データCRL1をサービスプロバイダ310に送信する(図102中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERCPの有効性を判断し、有効であると判断した場合に公開鍵データKCP、Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【0459】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図102中(1)、(2))。SAM3051は、サービスプロバイダ310から入力したセキュリティコンテンツ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データCRL1を参照して公開鍵証明書データCERCPの有効性を判断し、有効であると判断した場合に公開鍵データKCP、Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュリティコンテンツを無効にする。なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL1を、ユーザホームネットワーク303b内のネットワーク機器を介してSAM3051に直接送信してもよい(図102中(3))。

【0460】次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データCERSPを無効にする場合について説明する。図103に示すように、EMDサービスセンタ302は、公開鍵証明書データCERSPを無効にすることを示す公開鍵証明書破棄データCRL2をコンテンツプロバイダ301に送信する(図103中(1))。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データCRL2を参照して公開鍵証明書データCERSPの有効性を判断し、有効であると判断した場合に公開鍵データKSP、Pを用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

【0461】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL2を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM3051に送信する(図103中(2))。SAM3051は、サービスプロバイダ31

161

0から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER₂の有効性を判断し、有効であると判断した場合に公開鍵データK₂を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305に直接送信してもよい(図103中(3))。

【0462】次に、EMDサービスセンタ302が、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にする場合について説明する。図104に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃をコンテンツプロバイダ301に送信する(図104中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に公開鍵証明書破棄データCRL₃を送信する(図104中(1))。SAM305₁は、SAM305₂から入力したデータに付加されたSAM305₂の署名データを検証する際に、公開鍵証明書破棄データCRL₃を参照して公開鍵証明書データCER_{SAM2}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SAM2}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

【0463】EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい(図104中(1)、(2))。また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を、ユーザホームネットワーク303内のネットワーク機器を介してSA

162

M305₁に直接送信してもよい(図104中(3))。

【0464】また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃を作成し、これを保管する。また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図105中

(1))。EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図105中(1))。SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許可するか否かを決定する。

【0465】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをコンテンツプロバイダ301に送信する(図105中(2))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する(図105中(2))。次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する(図105中(2))。SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許可するか否かを決定する。

【0466】また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する(図105中(3))。次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する(図105中(3))。SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例え

163

ばSAM3052)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。以後、SAM3051は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許可するか否かを決定する。

【0467】EMDサービスセンタ302の役割等
図106は、図59に示すEMDサービスセンタ(クリアリングハウス)302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理(利益分配処理)を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

【0468】また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。また、コンテンツプロバイダ301の権利書データ106およびコンテンツ権データKCの登録(権威化)などを行う。なお、図107に示すように、権利管理用クリアリングハウス950と電子決済用クリアリングハウス951とを単体の装置内に収納すると、図59に示すEMDサービスセンタ302となる。

【0469】また、本発明は、例えば、図108に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス950の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス960からの決済請求権データに基づいて決済を行う。

【0470】また、本発明は、例えば、図109に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス970の機能を設け、権利管理用クリアリングハウス970において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてコンテンツプロバイダ301の決済請求権データを作成し、これをコンテンツプロバイダ301に送信してもよい。この場合には、コンテンツプロバイ

164

ダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970からの決済請求権データに基づいて決済を行う。

【0471】また、本発明は、例えば、図110に示すように、コンテンツプロバイダ301内に、前述した権利管理用クリアリングハウス970および電子決済用クリアリングハウス971の機能を備えるようにしてもよい。この場合には、コンテンツプロバイダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970において生成した決済請求権データに基づいて、決済機関91に対して自ら決済を行う。

【0472】第2実施形態の第8変形例

上述した第2実施形態では、図59に示すEMDシステム300において、コンテンツプロバイダ301からサービスプロバイダ310に図5に示すフォーマットのセキュアコンテナ104を提供し、サービスプロバイダ310からユーザホームネットワーク303に図65に示すフォーマットのセキュアコンテナ304を供給する場合を例示した。すなわち、上述した第2実施形態では、図5および図65に示すように、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ単数のコンテンツファイルCFと、当該コンテンツファイルCFに対応する単数のキーファイルKFを格納した場合を例示した。本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFにそれぞれ対応する複数のキーファイルKFとを格納してもよい。

【0473】図111は、本変形例において、図59に示すコンテンツプロバイダ301からサービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。図111に示すように、セキュアコンテナ104aには、コンテンツファイルCF₁、CF₂、CF₃、キーファイルKF₁、KF₂、KF₃、公開鍵証明書データCERT、署名データSIG₂₀₀、CF₁、SIG₂₀₁、CF₂、SIG₂₀₂、CF₃、SIG₂₀₃、CF₁、SIG₂₀₄、CF₂、SIG₂₀₅、CF₁、SIG₂₀₆、CF₂、SIG₂₀₇、CF₁、SIG₂₀₈、CF₂、SIG₂₀₉、CF₁、SIG₂₁₀、CF₂、SIG₂₁₁、CF₁、SIG₂₁₂、CF₂、SIG₂₁₃、CF₁、SIG₂₁₄、CF₂、SIG₂₁₅、CF₁、SIG₂₁₆、CF₂、SIG₂₁₇、CF₁、SIG₂₁₈、CF₂、SIG₂₁₉、CF₁、SIG₂₂₀、CF₂、SIG₂₂₁、CF₁、SIG₂₂₂、CF₂、SIG₂₂₃、CF₁、SIG₂₂₄、CF₂、SIG₂₂₅、CF₁、SIG₂₂₆、CF₂、SIG₂₂₇、CF₁、SIG₂₂₈、CF₂、SIG₂₂₉、CF₁、SIG₂₃₀、CF₂、SIG₂₃₁、CF₁、SIG₂₃₂、CF₂、SIG₂₃₃、CF₁、SIG₂₃₄、CF₂、SIG₂₃₅、CF₁、SIG₂₃₆、CF₂、SIG₂₃₇、CF₁、SIG₂₃₈、CF₂、SIG₂₃₉、CF₁、SIG₂₄₀、CF₂、SIG₂₄₁、CF₁、SIG₂₄₂、CF₂、SIG₂₄₃、CF₁、SIG₂₄₄、CF₂、SIG₂₄₅、CF₁、SIG₂₄₆、CF₂、SIG₂₄₇、CF₁、SIG₂₄₈、CF₂、SIG₂₄₉、CF₁、SIG₂₅₀、CF₂、SIG₂₅₁、CF₁、SIG₂₅₂、CF₂、SIG₂₅₃、CF₁、SIG₂₅₄、CF₂、SIG₂₅₅、CF₁、SIG₂₅₆、CF₂、SIG₂₅₇、CF₁、SIG₂₅₈、CF₂、SIG₂₅₉、CF₁、SIG₂₆₀、CF₂、SIG₂₆₁、CF₁、SIG₂₆₂、CF₂、SIG₂₆₃、CF₁、SIG₂₆₄、CF₂、SIG₂₆₅、CF₁、SIG₂₆₆、CF₂、SIG₂₆₇、CF₁、SIG₂₆₈、CF₂、SIG₂₆₉、CF₁、SIG₂₇₀、CF₂、SIG₂₇₁、CF₁、SIG₂₇₂、CF₂、SIG₂₇₃、CF₁、SIG₂₇₄、CF₂、SIG₂₇₅、CF₁、SIG₂₇₆、CF₂、SIG₂₇₇、CF₁、SIG₂₇₈、CF₂、SIG₂₇₉、CF₁、SIG₂₈₀、CF₂、SIG₂₈₁、CF₁、SIG₂₈₂、CF₂、SIG₂₈₃、CF₁、SIG₂₈₄、CF₂、SIG₂₈₅、CF₁、SIG₂₈₆、CF₂、SIG₂₈₇、CF₁、SIG₂₈₈、CF₂、SIG₂₈₉、CF₁、SIG₂₉₀、CF₂、SIG₂₉₁、CF₁、SIG₂₉₂、CF₂、SIG₂₉₃、CF₁、SIG₂₉₄、CF₂、SIG₂₉₅、CF₁、SIG₂₉₆、CF₂、SIG₂₉₇、CF₁、SIG₂₉₈、CF₂、SIG₂₉₉、CF₁、SIG₃₀₀、CF₂、SIG₃₀₁、CF₁、SIG₃₀₂、CF₂、SIG₃₀₃、CF₁、SIG₃₀₄、CF₂、SIG₃₀₅、CF₁、SIG₃₀₆、CF₂、SIG₃₀₇、CF₁、SIG₃₀₈、CF₂、SIG₃₀₉、CF₁、SIG₃₁₀、CF₂、SIG₃₁₁、CF₁、SIG₃₁₂、CF₂、SIG₃₁₃、CF₁、SIG₃₁₄、CF₂、SIG₃₁₅、CF₁、SIG₃₁₆、CF₂、SIG₃₁₇、CF₁、SIG₃₁₈、CF₂、SIG₃₁₉、CF₁、SIG₃₂₀、CF₂、SIG₃₂₁、CF₁、SIG₃₂₂、CF₂、SIG₃₂₃、CF₁、SIG₃₂₄、CF₂、SIG₃₂₅、CF₁、SIG₃₂₆、CF₂、SIG₃₂₇、CF₁、SIG₃₂₈、CF₂、SIG₃₂₉、CF₁、SIG₃₃₀、CF₂、SIG₃₃₁、CF₁、SIG₃₃₂、CF₂、SIG₃₃₃、CF₁、SIG₃₃₄、CF₂、SIG₃₃₅、CF₁、SIG₃₃₆、CF₂、SIG₃₃₇、CF₁、SIG₃₃₈、CF₂、SIG₃₃₉、CF₁、SIG₃₄₀、CF₂、SIG₃₄₁、CF₁、SIG₃₄₂、CF₂、SIG₃₄₃、CF₁、SIG₃₄₄、CF₂、SIG₃₄₅、CF₁、SIG₃₄₆、CF₂、SIG₃₄₇、CF₁、SIG₃₄₈、CF₂、SIG₃₄₉、CF₁、SIG₃₅₀、CF₂、SIG₃₅₁、CF₁、SIG₃₅₂、CF₂、SIG₃₅₃、CF₁、SIG₃₅₄、CF₂、SIG₃₅₅、CF₁、SIG₃₅₆、CF₂、SIG₃₅₇、CF₁、SIG₃₅₈、CF₂、SIG₃₅₉、CF₁、SIG₃₆₀、CF₂、SIG₃₆₁、CF₁、SIG₃₆₂、CF₂、SIG₃₆₃、CF₁、SIG₃₆₄、CF₂、SIG₃₆₅、CF₁、SIG₃₆₆、CF₂、SIG₃₆₇、CF₁、SIG₃₆₈、CF₂、SIG₃₆₉、CF₁、SIG₃₇₀、CF₂、SIG₃₇₁、CF₁、SIG₃₇₂、CF₂、SIG₃₇₃、CF₁、SIG₃₇₄、CF₂、SIG₃₇₅、CF₁、SIG₃₇₆、CF₂、SIG₃₇₇、CF₁、SIG₃₇₈、CF₂、SIG₃₇₉、CF₁、SIG₃₈₀、CF₂、SIG₃₈₁、CF₁、SIG₃₈₂、CF₂、SIG₃₈₃、CF₁、SIG₃₈₄、CF₂、SIG₃₈₅、CF₁、SIG₃₈₆、CF₂、SIG₃₈₇、CF₁、SIG₃₈₈、CF₂、SIG₃₈₉、CF₁、SIG₃₉₀、CF₂、SIG₃₉₁、CF₁、SIG₃₉₂、CF₂、SIG₃₉₃、CF₁、SIG₃₉₄、CF₂、SIG₃₉₅、CF₁、SIG₃₉₆、CF₂、SIG₃₉₇、CF₁、SIG₃₉₈、CF₂、SIG₃₉₉、CF₁、SIG₄₀₀、CF₂、SIG₄₀₁、CF₁、SIG₄₀₂、CF₂、SIG₄₀₃、CF₁、SIG₄₀₄、CF₂、SIG₄₀₅、CF₁、SIG₄₀₆、CF₂、SIG₄₀₇、CF₁、SIG₄₀₈、CF₂、SIG₄₀₉、CF₁、SIG₄₁₀、CF₂、SIG₄₁₁、CF₁、SIG₄₁₂、CF₂、SIG₄₁₃、CF₁、SIG₄₁₄、CF₂、SIG₄₁₅、CF₁、SIG₄₁₆、CF₂、SIG₄₁₇、CF₁、SIG₄₁₈、CF₂、SIG₄₁₉、CF₁、SIG₄₂₀、CF₂、SIG₄₂₁、CF₁、SIG₄₂₂、CF₂、SIG₄₂₃、CF₁、SIG₄₂₄、CF₂、SIG₄₂₅、CF₁、SIG₄₂₆、CF₂、SIG₄₂₇、CF₁、SIG₄₂₈、CF₂、SIG₄₂₉、CF₁、SIG₄₃₀、CF₂、SIG₄₃₁、CF₁、SIG₄₃₂、CF₂、SIG₄₃₃、CF₁、SIG₄₃₄、CF₂、SIG₄₃₅、CF₁、SIG₄₃₆、CF₂、SIG₄₃₇、CF₁、SIG₄₃₈、CF₂、SIG₄₃₉、CF₁、SIG₄₄₀、CF₂、SIG₄₄₁、CF₁、SIG₄₄₂、CF₂、SIG₄₄₃、CF₁、SIG₄₄₄、CF₂、SIG₄₄₅、CF₁、SIG₄₄₆、CF₂、SIG₄₄₇、CF₁、SIG₄₄₈、CF₂、SIG₄₄₉、CF₁、SIG₄₅₀、CF₂、SIG₄₅₁、CF₁、SIG₄₅₂、CF₂、SIG₄₅₃、CF₁、SIG₄₅₄、CF₂、SIG₄₅₅、CF₁、SIG₄₅₆、CF₂、SIG₄₅₇、CF₁、SIG₄₅₈、CF₂、SIG₄₅₉、CF₁、SIG₄₆₀、CF₂、SIG₄₆₁、CF₁、SIG₄₆₂、CF₂、SIG₄₆₃、CF₁、SIG₄₆₄、CF₂、SIG₄₆₅、CF₁、SIG₄₆₆、CF₂、SIG₄₆₇、CF₁、SIG₄₆₈、CF₂、SIG₄₆₉、CF₁、SIG₄₇₀、CF₂、SIG₄₇₁、CF₁、SIG₄₇₂、CF₂、SIG₄₇₃、CF₁、SIG₄₇₄、CF₂、SIG₄₇₅、CF₁、SIG₄₇₆、CF₂、SIG₄₇₇、CF₁、SIG₄₇₈、CF₂、SIG₄₇₉、CF₁、SIG₄₈₀、CF₂、SIG₄₈₁、CF₁、SIG₄₈₂、CF₂、SIG₄₈₃、CF₁、SIG₄₈₄、CF₂、SIG₄₈₅、CF₁、SIG₄₈₆、CF₂、SIG₄₈₇、CF₁、SIG₄₈₈、CF₂、SIG₄₈₉、CF₁、SIG₄₉₀、CF₂、SIG₄₉₁、CF₁、SIG₄₉₂、CF₂、SIG₄₉₃、CF₁、SIG₄₉₄、CF₂、SIG₄₉₅、CF₁、SIG₄₉₆、CF₂、SIG₄₉₇、CF₁、SIG₄₉₈、CF₂、SIG₄₉₉、CF₁、SIG₅₀₀、CF₂、SIG₅₀₁、CF₁、SIG₅₀₂、CF₂、SIG₅₀₃、CF₁、SIG₅₀₄、CF₂、SIG₅₀₅、CF₁、SIG₅₀₆、CF₂、SIG₅₀₇、CF₁、SIG₅₀₈、CF₂、SIG₅₀₉、CF₁、SIG₅₁₀、CF₂、SIG₅₁₁、CF₁、SIG₅₁₂、CF₂、SIG₅₁₃、CF₁、SIG₅₁₄、CF₂、SIG₅₁₅、CF₁、SIG₅₁₆、CF₂、SIG₅₁₇、CF₁、SIG₅₁₈、CF₂、SIG₅₁₉、CF₁、SIG₅₂₀、CF₂、SIG₅₂₁、CF₁、SIG₅₂₂、CF₂、SIG₅₂₃、CF₁、SIG₅₂₄、CF₂、SIG₅₂₅、CF₁、SIG₅₂₆、CF₂、SIG₅₂₇、CF₁、SIG₅₂₈、CF₂、SIG₅₂₉、CF₁、SIG₅₃₀、CF₂、SIG₅₃₁、CF₁、SIG₅₃₂、CF₂、SIG₅₃₃、CF₁、SIG₅₃₄、CF₂、SIG₅₃₅、CF₁、SIG₅₃₆、CF₂、SIG₅₃₇、CF₁、SIG₅₃₈、CF₂、SIG₅₃₉、CF₁、SIG₅₄₀、CF₂、SIG₅₄₁、CF₁、SIG₅₄₂、CF₂、SIG₅₄₃、CF₁、SIG₅₄₄、CF₂、SIG₅₄₅、CF₁、SIG₅₄₆、CF₂、SIG₅₄₇、CF₁、SIG₅₄₈、CF₂、SIG₅₄₉、CF₁、SIG₅₅₀、CF₂、SIG₅₅₁、CF₁、SIG₅₅₂、CF₂、SIG₅₅₃、CF₁、SIG₅₅₄、CF₂、SIG₅₅₅、CF₁、SIG₅₅₆、CF₂、SIG₅₅₇、CF₁、SIG₅₅₈、CF₂、SIG₅₅₉、CF₁、SIG₅₆₀、CF₂、SIG₅₆₁、CF₁、SIG₅₆₂、CF₂、SIG₅₆₃、CF₁、SIG₅₆₄、CF₂、SIG₅₆₅、CF₁、SIG₅₆₆、CF₂、SIG₅₆₇、CF₁、SIG₅₆₈、CF₂、SIG₅₆₉、CF₁、SIG₅₇₀、CF₂、SIG₅₇₁、CF₁、SIG₅₇₂、CF₂、SIG₅₇₃、CF₁、SIG₅₇₄、CF₂、SIG₅₇₅、CF₁、SIG₅₇₆、CF₂、SIG₅₇₇、CF₁、SIG₅₇₈、CF₂、SIG₅₇₉、CF₁、SIG₅₈₀、CF₂、SIG₅₈₁、CF₁、SIG₅₈₂、CF₂、SIG₅₈₃、CF₁、SIG₅₈₄、CF₂、SIG₅₈₅、CF₁、SIG₅₈₆、CF₂、SIG₅₈₇、CF₁、SIG₅₈₈、CF₂、SIG₅₈₉、CF₁、SIG₅₉₀、CF₂、SIG₅₉₁、CF₁、SIG₅₉₂、CF₂、SIG₅₉₃、CF₁、SIG₅₉₄、CF₂、SIG₅₉₅、CF₁、SIG₅₉₆、CF₂、SIG₅₉₇、CF₁、SIG₅₉₈、CF₂、SIG₅₉₉、CF₁、SIG₆₀₀、CF₂、SIG₆₀₁、CF₁、SIG₆₀₂、CF₂、SIG₆₀₃、CF₁、SIG₆₀₄、CF₂、SIG₆₀₅、CF₁、SIG₆₀₆、CF₂、SIG₆₀₇、CF₁、SIG₆₀₈、CF₂、SIG₆₀₉、CF₁、SIG₆₁₀、CF₂、SIG₆₁₁、CF₁、SIG₆₁₂、CF₂、SIG₆₁₃、CF₁、SIG₆₁₄、CF₂、SIG₆₁₅、CF₁、SIG₆₁₆、CF₂、SIG₆₁₇、CF₁、SIG₆₁₈、CF₂、SIG₆₁₉、CF₁、SIG₆₂₀、CF₂、SIG₆₂₁、CF₁、SIG₆₂₂、CF₂、SIG₆₂₃、CF₁、SIG₆₂₄、CF₂、SIG₆₂₅、CF₁、SIG₆₂₆、CF₂、SIG₆₂₇、CF₁、SIG₆₂₈、CF₂、SIG₆₂₉、CF₁、SIG₆₃₀、CF₂、SIG₆₃₁、CF₁、SIG₆₃₂、CF₂、SIG₆₃₃、CF₁、SIG₆₃₄、CF₂、SIG₆₃₅、CF₁、SIG₆₃₆、CF₂、SIG₆₃₇、CF₁、SIG₆₃₈、CF₂、SIG₆₃₉、CF₁、SIG₆₄₀、CF₂、SIG₆₄₁、CF₁、SIG₆₄₂、CF₂、SIG₆₄₃、CF₁、SIG₆₄₄、CF₂、SIG₆₄₅、CF₁、SIG₆₄₆、CF₂、SIG₆₄₇、CF₁、SIG₆₄₈、CF₂、SIG₆₄₉、CF₁、SIG₆₅₀、CF₂、SIG₆₅₁、CF₁、SIG₆₅₂、CF₂、SIG₆₅₃、CF₁、SIG₆₅₄、CF₂、SIG₆₅₅、CF₁、SIG₆₅₆、CF₂、SIG₆₅₇、CF₁、SIG₆₅₈、CF₂、SIG₆₅₉、CF₁、SIG₆₆₀、CF₂、SIG₆₆₁、CF₁、SIG₆₆₂、CF₂、SIG₆₆₃、CF₁、SIG₆₆₄、CF₂、SIG₆₆₅、CF₁、SIG₆₆₆、CF₂、SIG₆₆₇、CF₁、SIG₆₆₈、CF₂、SIG₆₆₉、CF₁、SIG₆₇₀、CF₂、SIG₆₇₁、CF₁、SIG₆₇₂、CF₂、SIG₆₇₃、CF₁、SIG₆₇₄、CF₂、SIG₆₇₅、CF₁、SIG₆₇₆、CF₂、SIG₆₇₇、CF₁、SIG₆₇₈、CF₂、SIG₆₇₉、CF₁、SIG₆₈₀、CF₂、SIG₆₈₁、CF₁、SIG₆₈₂、CF₂、SIG₆₈₃、CF₁、SIG₆₈₄、CF₂、SIG₆₈₅、CF₁、SIG₆₈₆、CF₂、SIG₆₈₇、CF₁、SIG₆₈₈、CF₂、SIG₆₈₉、CF₁、SIG₆₉₀、CF₂、SIG₆₉₁、CF₁、SIG₆₉₂、CF₂、SIG₆₉₃、CF₁、SIG₆₉₄、CF₂、SIG₆₉₅、CF₁、SIG₆₉₆、CF₂、SIG₆₉₇、CF₁、SIG₆₉₈、CF₂、SIG₆₉₉、CF₁、SIG₇₀₀、CF₂、SIG₇₀₁、CF₁、SIG₇₀₂、CF₂、SIG₇₀₃、CF₁、SIG₇₀₄、CF₂、SIG₇₀₅、CF₁、SIG₇₀₆、CF₂、SIG₇₀₇、CF₁、SIG₇₀₈、CF₂、SIG₇₀₉、CF₁、SIG₇₁₀、CF₂、SIG₇₁₁、CF₁、SIG₇₁₂、CF₂、SIG₇₁₃、CF₁、SIG₇₁₄、CF₂、SIG₇₁₅、CF₁、SIG₇₁₆、CF₂、SIG₇₁₇、CF₁、SIG₇₁₈、CF₂、SIG₇₁₉、CF₁、SIG₇₂₀、CF₂、SIG₇₂₁、CF₁、SIG₇₂₂、CF₂、SIG₇₂₃、CF₁、SIG₇₂₄、CF₂、SIG₇₂₅、CF₁、SIG₇₂₆、CF₂、SIG₇₂₇、CF₁、SIG₇₂₈、CF₂、SIG₇₂₉、CF₁、SIG₇₃₀、CF₂、SIG₇₃₁、CF₁、SIG₇₃₂

165

メタデータMet a1、コンテンツデータC1、A/V伸長用ソフトウェアSof t1および電子透かし情報モジュールWM1が格納されている。ここで、コンテンツデータC1およびA/V伸長用ソフトウェアSof t1は、コンテンツ鍵データKc1を用いて暗号化されており、メタデータMet a1および電子透かし情報モジュールWM1は必要に応じてコンテンツ鍵データKc1を用いて暗号化されている。また、コンテンツデータC1は、例えば、ATRAC3方式で圧縮されている。A/V伸長用ソフトウェアSof t1は、ATRAC3方式の伸長用のソフトウェアである。また、コンテンツファイルCF1のヘッダには、例えば、図112に示すようにキーファイルKF1およびコンテンツファイルCF2にリンクすることを示すディレクトリ構造データDSD1が含まれている。

【0475】コンテンツファイルCF2には、ヘッダ、メタデータMet a2、コンテンツデータC2、A/V伸長用ソフトウェアSof t2および電子透かし情報モジュールWM2が格納されている。ここで、コンテンツデータC2およびA/V伸長用ソフトウェアSof t2は、コンテンツ鍵データKc2を用いて暗号化されており、メタデータMet a2および電子透かし情報モジュールWM2は必要に応じてコンテンツ鍵データKc2を用いて暗号化されている。また、コンテンツデータC2は、例えば、MPEG2方式で圧縮されている。A/V伸長用ソフトウェアSof t2は、MPEG2方式の伸長用のソフトウェアである。また、コンテンツファイルCF2のヘッダには、例えば、図112に示すように、キーファイルKF2およびコンテンツファイルCF3にリンクすることを示すディレクトリ構造データDSD2

【0476】コンテンツファイルCF3には、ヘッダ、メタデータMet a3、コンテンツデータC3、A/V伸長用ソフトウェアSof t3および電子透かし情報モジュールWM3が格納されている。ここで、コンテンツデータC3およびA/V伸長用ソフトウェアSof t3は、コンテンツ鍵データKc3を用いて暗号化されており、メタデータMet a3および電子透かし情報モジュールWM3は必要に応じてコンテンツ鍵データKc3を用いて暗号化されている。また、コンテンツデータC3は、例えば、JPEG方式で圧縮されている。A/V伸長用ソフトウェアSof t3は、JPEG方式の伸長用のソフトウェアである。また、コンテンツファイルCF3のヘッダには、例えば、図112に示すように、キーファイルKF3にリンクすることを示すディレクトリ構造データDSD3が含まれている。

【0477】キーファイルKF1には、ヘッダと、配信鍵データKD1〜KD3を用いて暗号化されたコンテンツ鍵データKc1、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1と、署名

166

データSIG220、ESCとが格納されている。

【0478】キーファイルKF2には、ヘッダと、配信鍵データKD2〜KD3を用いて暗号化されたコンテンツ鍵データKc2、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC2と、署名データSIG221、ESCとが格納されている。

【0479】キーファイルKF3には、ヘッダと、配信鍵データKD3〜KD3を用いて暗号化されたコンテンツ鍵データKc3、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC3と、署名データSIG222、ESCとが格納されている。

【0480】サービスプロバイダ310は、図112に示すセキュアコンテナ304aの配給を受けると、EMDサービスセンタ302の公開鍵データKesc、pを用いて公開鍵証明書データCERcpの正当性を確認した後に、当該公開鍵証明書データCERcpに格納された公開鍵データKcp、pを用いて、署名データSIG200、CP、SIG201、CP、SIG202、CP、SIG203、CP、SIG204、CP、SIG205、CPの正当性、すなわちコンテンツファイルCF1、CF2、CF3の作成者および送信者の正当性と、キーファイルKF1、KF2、KF3の送信者の正当性を確認する。また、コンテンツプロバイダ301は、公開鍵データKesc、pを用いて、署名データSIG220、ESC、SIG221、ESC、SIG222、ESCの正当性、キーファイルKF1、KF2、KF3の作成者の正当性を確認する。

【0481】そして、サービスプロバイダ310は、コンテンツファイルCF1、CF2、CF3の販売価格を示すプライスタグデータ3121、3122、3123を作成する。また、サービスプロバイダ310は、秘密鍵データKsp、sを用いて、プライスタグデータ3121、3122、3123の署名データSIG220、SP、SIG221、SP、SIG222、SPを作成する。また、サービスプロバイダ310は、秘密鍵データKsp、sを用いて、コンテンツファイルCF1、CF2、CF3、KF1、KF2、KF3の署名データSIG210、SP、SIG211、SP、SIG212、SP、SIG213、SP、SIG214、SP、SIG215、SPを作成する。

【0482】次に、サービスプロバイダ310は、図114に示すセキュアコンテナ304sを作成する。

【0483】サービスプロバイダ310は、図114に示すセキュアコンテナ304aをユーザホームネットワーク303に配給する。ユーザホームネットワーク303では、SAM3051〜3054において、セキュアコンテナ304aに格納された全ての署名データの正当性を確認した後に、コンテンツデータC1、C2、C3

167

についての権利処理を、ディレクトリ構造データDSD₁〜DSD_nに示されるリンク状態に応じて、それぞれキーファイルKF₁、KF₂、KF₃に基づいて行う。

【0484】また、上述した第8変形例では、セキュアコンテナ304において、単数のサービスプロバイダ301から提供を受けた複数のコンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃を単数のセキュアコンテナ304aに格納しユーザホームネットワーク303に配給する場合を例示したが、図98に示すように、複数のコンテンツプロバイダ301a、301bから提供を受けた複数のコンテンツファイルCFを、単数のセキュアコンテナに格納してユーザホームネットワーク303に配給してもよい。

【0485】また、セキュアコンテナ104、304内には、例えば、図113に示すように、ATRAC3で圧縮された楽曲（音声）データを格納したコンテンツファイルCF₁、MP3で圧縮されたビデオクリップデータを格納したコンテンツファイルCF₂、JPEGで圧縮されたジャケット（静止画）データを格納したコンテンツファイルCF₃、オーディオ形式の歌詞データを格納したコンテンツファイルCF₄、並びにテキスト形式のライナーノーツデータを格納したコンテンツファイルCF₅と、それぞれに対応したキーファイルKF₁、KF₂、KF₃、KF₄、KF₅とを格納してもよい。この場合にも、同様に、コンテンツファイルCF₁〜CF₅のディレクトリ構造データによって、コンテンツファイルCF₁〜CF₅と相互間のリンクと、コンテンツファイルCF₁〜CF₅とキーファイルKF₁〜KF₅との間のそれぞれのリンクとが確立される。

【0486】なお、本実施形態におけるセキュアコンテナ内に複数のコンテンツデータを格納する場合（コンポジット型の場合）のデータフォーマットの概念は、例えば、図115あるいは図116に示される。

【0487】なお、図111に示すフォーマットは、前述した第1実施形態において、図1に示すコンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を送信する場合にも同様に適用できる。

【0488】第2実施形態の第9変形例

上述した実施形態では、コンテンツファイルCFおよびキーファイルKFをディレクトリ構造でセキュアコンテナ104、304に格納してコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁〜305_nに送信する場合を例示したが、コンテンツファイルCFおよびキーファイルKFを、別々にコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁〜305_nに送信してもよい。これには、例えば、以下に示す第1の手法と第2の手法とがある。第1の手法では、図117に示すよう

168

に、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁〜305_nに、コンテンツファイルCFおよびキーファイルKFを別々に送信する。また、第2の手法では、図118に示すように、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁〜305_nにコンテンツファイルCFを送信し、EMDサービスセンタ302からSAM305₁〜305_nにキーファイルKFを送信する。当該キーファイルKFの送信は、例えば、SAM305₁〜305_nのユーザが、コンテンツデータCの購入形態を決定しようとするときに、EMDサービスセンタ302からSAM305₁〜305_nに送信される。上述した第1の手法および第2の手法を採用する場合には、例えば、関連するコンテンツファイルCF相互間と、コンテンツファイルCFとそれに対応するキーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータHLを用いてリンク関係を確立する。SAM105₁〜105_nでは、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。

【0489】また、上述した第2実施形態では、コンテンツデータCと、コンテンツ鍵データKcおよび権利書データC6などの鍵データとをそれぞれファイル形式にして、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁〜305_nに送信する場合を例示したが、これらは、相互間でのリンク関係が確立できれば、必ずしもファイル形式にする必要はない。例えば、図119に示すように、コンテンツデータC、メタデータMeta、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーファイルKF、ブライスタグデータ312および、公開鍵証明書データCERcr、CERsrを別々に、コンテンツプロバイダ301およびEMDサービスセンタ302からSAM305₁〜305_nに送信してもよい。この場合には、図119に示すように、コンテンツデータC、メタデータMeta、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーファイルKF、ブライスタグデータ312、公開鍵証明書データCERcr、CERsrが、ハイパーリンクデータHLによってリンクされる。ここで、ハイパーリンクデータHLは、例えば、配信用鍵データKD₁〜KD_nで暗号化されて送信される。

【0490】なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5（A）、（B）に示すものが採用される。また、この場合にも、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データS1

G6、CP、SIG7、CPを送信することが好ましい。

【0491】第2実施形態の第10変形例

上述した実施形態では、セキュアコンテナ104内において、コンテンツファイルCFおよびキーファイルKFを別々に設けた場合を例示したが、例えば、図120に示すように、セキュアコンテナ104、304内において、コンテンツファイルCF内にキーファイルKFを格納するようにしてもよい。この場合に、キーファイルKFを格納したコンテンツファイルCFに対して、コンテンツプロバイダ301の秘密鍵データKcp、sによる署名データKsp、sによる署名データが付される。

第2実施形態の第11変形例

上述した実施形態では、コンテンツデータCをコンテンツファイルCFに格納し、コンテンツ鍵データKcおよび権利書データ106をキーファイルKF内に格納してコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM3051などに送信する場合を例示したが、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM3051などに、通信プロトコルに依存しない形式で送信してもよい。

【0492】例えば、図121に示すように、コンテンツプロバイダ301において、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106を含むキーファイルKFとを格納したセキュアコンテナ104sを作成し、セキュアコンテナ104sをサービスプロバイダ310に通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ310において、セキュアコンテナ104sに格納されたコンテンツデータCおよびキーファイルKFにプライスタグデータ312を加えてセキュアコンテナ304sを作成し、セキュアコンテナ304sをSAM3051などに通信プロトコルに依存しない形式で送信してもよい。

【0593】また、図122に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを通信プロトコルに依存しない形式で個別に送信する。そして、サービスプロバイダ310からSAM3051などに、コンテンツデータC、キーファイルKFおよびプライスタグデータ312を通信プロトコルに依存しない形式で個別に送信する。すなわち、コンテンツデ

ータCをファイル形式にしないで、キーファイルKFと同一経路で送信する。

【0494】また、図123に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCを通信プロトコルに依存しない形式で送信し、サービスプロバイダ310からSAM3051などにコンテンツデータCおよびプライスタグデータ312を通信プロトコルに依存しない形式で送信する。また、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFをEMDサービスセンタ302からSAM3051などに送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと別経路で送信する。

【0495】また、図124に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信する。また、サービスプロバイダ310からSAM3051などに、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106、並びにプライスタグデータ312を送信する。すなわち、コンテンツデータC、コンテンツ鍵データKc、権利書データ106およびプライスタグデータ312をファイル形式にしないで、同一経路で送信する。

【0496】また、図125に示すように、コンテンツプロバイダ301からサービスプロバイダ310に、コンテンツ鍵データKcで暗号化されたコンテンツデータCを、通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ310からSAM3051などに、コンテンツデータCおよびプライスタグデータ312を、通信プロトコルに依存しない形式で送信する。また、EMDサービスセンタ302からSAM3051などにコンテンツ鍵データKcおよび権利書データ106を送信する。すなわち、コンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とをファイル形式にしないで、別経路で送信する。

【0497】第2実施形態の第12変形例

前述した図59に示すEMDシステム300では、例えば、図126に示すように、ユーザホームネットワーク303がサービスプロバイダ310から受信したセキュアコンテナ304に応じたセキュアコンテナ304Aを、ユーザホームネットワーク303aのSAMからの要求S303aに応じて、ユーザホームネットワーク303aに配給してもよい。この場合には、ユーザホームネットワーク303のSAMが、前述した第2実施形態で説明したサービスプロバイダ310と同様の役割を果たすと考えられることができる。この場合に、ユーザホームネットワーク303aのSAMは、独自にプライスタグ

171

データ312を新たに設定できる。そして、ユーザホームネットワーク303aのSAMにおいてコンテンツデータCの購入形態が決定され、それに応じた利用履歴データ304aなどがユーザホームネットワーク303aのSAMからEMDサービスセンタ302に送信される。EMDサービスセンタ302では、利用履歴データ304aに基づいて、コンテンツプロバイダ301、サービスプロバイダ310、ユーザホームネットワーク303のユーザに、ユーザホームネットワーク303aのユーザが支払った金銭を分配するための決済処理を行う。

【0498】なお、本実施形態におけるセキュアコンテンツのファイル包括大小関係は、図127に示すように表現できる。

【0499】第3実施形態

図128は本発明の第3実施形態のEMDシステムを説明するための図、図129は図128に示すEMDサービスセンタの機能ブロック図である。図129において、前述した第1実施形態および第2実施形態で用いた符号と同じ符号を付した構成要素は、これらの実施形態で説明した同一符号の構成要素と同じである。

【0500】本実施形態のEMDシステムでは、コンテンツプロバイダ301はMDサービスセンタ302にマスタソース（コンテンツデータ）S111などを送り、EMDサービスセンタ302において例えば図5（A）に示すコンテンツファイルCFを作成する。また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータS111のコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの転売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。また、EMDサービスセンタ302は、作成したコンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、キーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

【0501】EMDサービスセンタ302における処理を図129を参照して説明する。EMDサービスセンタ302は、コンテンツプロバイダ301から受け取ったマスタソースS111をコンテンツマスタソースデータベース801に格納する。次に、電子透かし情報付加部112において、コンテンツプロバイダ301から受け取った電子透かし管理情報を示す電子透かし情報を、コンテンツマスタソースデータベース801から読み出し

172

たマスタソースS111に埋め込んでコンテンツデータS112を生成する。次に、圧縮部113において、コンテンツデータS112を圧縮してコンテンツデータS113を生成する。コンテンツデータS112は、伸長部116において伸長された後に、聴感検査部123において聴感検査が行われ、必要であれば、電子透かし情報付加部112において電子透かし情報が再び埋め込まれる。次に、暗号化部114において、コンテンツデータS113がコンテンツ鍵データKcを用いて暗号化されてコンテンツデータS114が生成される。次に、CF作成部802において、コンテンツデータS114などを格納した図5（A）に示すコンテンツファイルCFが作成され、コンテンツファイルCFがCFデータベース802aに格納される。

【0502】また、EMDサービスセンタ302では、KF作成部153において、図5（B）に示すキーファイルKFを作成し、キーファイルKFをKFデータベース153aに格納する。

【0503】次に、セキュアコンテンツ作成部804において、CFデータベース802aから読み出したコンテンツファイルCFと、KFデータベース153aから読み出したキーファイルKFとを格納したセキュアコンテンツ806が作成され、セキュアコンテンツ806がセキュアコンテンツデータベース805に格納される。その後、セキュアコンテンツデータベース805が、サービスプロバイダ310によってアクセスされて、セキュアコンテンツ806がサービスプロバイダ310に供給される。

【0504】次に、サービスプロバイダ310は、セキュアコンテンツ806に格納されたコンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテンツ807を作成する。そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテンツ807をユーザホームネットワーク303に配給する。

【0505】ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテンツ807がSAM305iなどに提供され、SAM305iなどにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD_i〜KD_nなどを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、SAM305iなどにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。また、ユーザホームネットワーク303のSAM305iから、ユーザホームネットワーク303aのS

173

AM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

【0506】なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。また、図128に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図130に示すように、EMDサービスセンタ302において作成したコンテンツファイルCFをサービスプロバイダ310に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₂、SAM305₁₂に供給してもよい。

【0507】第4実施形態

図131は本発明の第4実施形態のEMDシステムを説明するための図である。

【0508】本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5（A）に示すコンテンツファイルCFを作成し、これをEMDサービスセンタ302に送る。また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ301の識別子C_P_ID、コンテンツデータを提供するサービスプロバイダ310の識別子S_P_ID、コンテンツデータの著作権SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。また、EMDサービスセンタ302は、コンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、作成したキーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

【0509】また、EMDサービスセンタ302では、

174

CFデータベース802aから読み出したコンテンツファイルCFと、KFデータベース153aから読み出したキーファイルKFとを格納したセキュアコンテナ806が作成され、セキュアコンテナ806がセキュアコンテナデータベースに格納される。その後、セキュアコンテナデータベースが、サービスプロバイダ310によってアクセスされて、セキュアコンテナ806がサービスプロバイダ310に供給される。

【0510】次に、サービスプロバイダ310は、セキュアコンテナ806に格納されたコンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテナ807を作成する。そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテナ807をユーザホームネットワーク303に配給する。

【0511】ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ807がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁～KD₃などを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

【0512】なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。また、図131に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図132に示すように、コンテンツファイルCFをEMDサービスセンタ302からサービスプロバイダ3

175

10に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₂、SAM305₁₂に供給してもよい。

【0513】第5実施形態

図133は本発明の第5実施形態のEMDシステムを説明するための図である。

【0514】本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5(A)に示すコンテンツファイルCFを作成する。また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報(コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報)、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5(B)に示すキーファイルKFを作成する。EMDサービスセンタ302は、作成したキーファイルKFをコンテンツプロバイダ301に送る。また、EMDサービスセンタ302は、KFデータベース153aにキーファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてキーファイルKFを一元的に管理する。このとき、コンテンツIDは、例えば、EMDサービスセンタ302によって作成され、複数のコンテンツプロバイダ301が提供するコンテンツデータの全てを対象としてグローバルユニークに決定される。

【0515】次に、コンテンツプロバイダ301において、作成したコンテンツファイルCFと、EMDサービスセンタ302から受けたキーファイルKFとを格納したセキュアコンテナ821が作成され、セキュアコンテナ821が共通データベース820に格納される。共通データベース820において、複数のコンテンツプロバイダ301が提供したセキュアコンテナ821が、コンテンツIDを用いて一元的に管理される。

【0516】サービスプロバイダ310は、例えば、コンテンツIDを用いて共通データベース820をブライジング(検索)して、所望のセキュアコンテナ821を共通データベース820から受けて、セキュアコンテナ821に、コンテンツの販売価格を示すプライスタグデータ312などをさらに格納したセキュアコンテナ822を作成し、セキュアコンテナ822をユーザホームネットワーク303に配給する。

【0517】ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ822がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに

176

格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKDiへKDiを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ822が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

【0518】なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対する処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。また、図133に示す例では、コンテンツプロバイダ301から共通データベース820、共通データベース820からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送る場合(イン・バンドの場合)を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい(アウト・オブ・バンドの場合)。また、図134に示すように、コンテンツプロバイダ301から共通データベース820にコンテンツファイルCFを格納し、サービスプロバイダ310が共通データベース820からコンテンツファイルCFを得ると共に、EMDサービスセンタ302からサービスプロバイダ310にキーファイルKFを送るようにしてもよい。この場合には、サービスプロバイダ310は、共通データベース820から得たコンテンツファイルCFと、EMDサービスセンタ302から得たキーファイルKFと、プライスタグデータ312とを格納してセキュアコンテナ822を作成する。共通データベース820は、複数のコンテンツプロバイダ301が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

【0519】また、図135に示すように、EMDサービスセンタ302が作成したキーファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。この場合には、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。プライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよい

177

し、EMDサービスセンタ302がユーザホームネットワーク303、303aに接続してもよい。

【0520】第6実施形態

図136は本発明の第6実施形態のEMDシステムを説明するための図である

【0521】本実施形態のEMDシステムは、前述した図133に示すEMDシステムと比較すると、複数のEMDサービスセンタ302を有し、コンテンツプロバイダ301がそれぞれ対応するEMDサービスセンタ302との間で課金処理などを行うことを特徴としている点

が異なり、それ以外の点は略同じである。コンテンツプロバイダ301は例えば図5(A)に示すコンテンツツ

ファイルCFを作成する。また、コンテンツプロバイダ301は、複数のEMDサービスセンタ302のうち自ら

が選択した(あるいは予め決められた)一のEMDサービスセンタ302に、コンテンツデータのコンテンツID、

コンテンツ鍵データKc、電子透かし管理情報(コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報)、コンテンツプロバイダ301の

識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの

販売価格SRPを送り、EMDサービスセンタ302において図5(B)に示すキーファイルKFを作成する。EMDサービスセンタ302は、作成したキー

ファイルKFを、対応するコンテンツプロバイダ301に送る。また、EMDサービスセンタ302は、KFデータ

ベース153aにキーファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてキーファイルKFを一元的に管理する。このとき、

コンテンツIDは、例えば、EMDサービスセンタ302によって作成され、共通データベース830に格納される全てのセキュアコンテナ831に対応するコンテンツ

データを対象としてグローバルユニークに決定される。

【0522】次に、コンテンツプロバイダ301において、作成したコンテンツファイルCFと、EMDサービスセンタ302から受けたキーファイルKFとを格納したセキュアコンテナ831が作成され、セキュアコンテナ831が共通データベース820に格納される。共通データベース830において、複数のコンテンツプロバイダ301が提供したセキュアコンテナ831が、コンテンツIDを用いて一元的に管理される。

【0523】サービスプロバイダ310は、例えば、コンテンツIDを用いて共通データベース820をブランチング(検索)して、希望のセキュアコンテナ831を

10

20

30

40

50

178

【0524】ユーザホームネットワーク303では、オンラインの場合にはCAキヨール311を介してセキュアコンテナ832がSAM3051などに提供され、SAM3051などにおいて、キーファイルKFに

格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD1〜KD3などを用いて復号され、復号された権利書データ106に基づいて、

コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、SAM3051などにおいて、コンテンツデータの購入履歴

などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。また、ユーザホームネットワーク303のSAM

3052から、ユーザホームネットワーク303aのSAM30512にセキュアコンテナ832が転送される場合には、SAM30512においてSAM3052と同様の処理が行われ、SAM30512からEMDサービスセンタ302に利用履歴データ308が送信される。

【0525】なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対する処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。また、図136に示す例では、

コンテンツプロバイダ301から共通データベース830、共通データベース830からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホーム

ネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送る場合(イン・バンドの場合)を例示したが、

コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい(アウト・オブ・バンドの場合)。また、図137に示すように、

コンテンツプロバイダ301から共通データベース830にコンテンツファイルCFを格納し、サービスプロバイダ310が共通データベース820からコンテンツファイルCFを得ると共に、

EMDサービスセンタ302からサービスプロバイダ310にキーファイルKFを送るようにしてもよい。このとき、サービスプロバイダ310が得たコンテンツ

ファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からサービスプロバイダ310にキーファイルKFが送られる。

【0526】サービスプロバイダ310は、共通データベース830から得たコンテンツファイルCFと、EMDサービスセンタ302から得たキーファイルKFと、

ブライスタグデータ312とを格納してセキュアコンテナ832を作成する。共通データベース830は、複数のコンテンツプロバイダ301が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理

する。

【0527】また、図138に示すように、EMDサービスセンタ302が作成したキープファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。このときも、SAM305₁、305₁₂などに提供されたコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からSAM305₁、305₁₂などにキープファイルKFが送られる。また、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。ブライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよいし、EMDサービスセンタ302がユーザホームネットワーク303、303aに配給してもよい。

【0528】第7実施形態

図139は本発明の第7実施形態のEMDシステムを説明するための図である。

【0529】本実施形態のEMDシステムは、前述した図136に示すEMDシステムと比較すると、コンテンツプロバイダ301からEMDサービスセンタ302にコンテンツデータのマスソースS111を送り、EMDサービスセンタ302においてコンテンツファイルCFを作成する点と異なり、それ以外の点は略同じである。コンテンツプロバイダ301は、コンテンツデータのマスソースS111を複数のEMDサービスセンタ302のうち自らが選択した（あるいは予め決められた）1のEMDサービスセンタ302に送り、EMDサービスセンタ302において、図5（A）に示すコンテンツファイルCFを作成する。EMDサービスセンタ302は、作成したコンテンツファイルCFを対応するコンテンツプロバイダ301に送る。

【0530】また、コンテンツプロバイダ301は、上記の対応するEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データK_c、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの販売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキープファイルKFを作成する。EMDサービスセンタ302は、作成したキープファイルKFを、対応するコンテンツプロバイダ301に送る。また、EMDサービスセンタ302は、CFデータベース802aにコンテンツファイルCFを格納し、KFデータベース153aにキープファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてコンテンツファイルCFおよびキープファイルKFを一元的に管理する。このとき、コンテンツIDは、例えば、EMDサービスセンタ302によって

作成され、共通データベース840に格納される全てのセキュアコンテンツ831に対応するコンテンツデータを対象としてグローバルユニークに決定される。

【0531】次に、コンテンツプロバイダ301において、対応するEMDサービスセンタ302から受けたコンテンツファイルCFおよびキープファイルKFとを格納したセキュアコンテンツ841が作成され、セキュアコンテンツ841が共通データベース840に格納される。共通データベース840において、複数のコンテンツプロバイダ301が提供したセキュアコンテンツ841が、コンテンツIDを用いて一元的に管理される。

【0532】サービスプロバイダ310は、例えば、コンテンツIDを用いて共通データベース840をブラウジング（検索）して、所望のセキュアコンテンツ841を共通データベース840から受けて、セキュアコンテンツ841に、コンテンツの販売価格を示すブライスタグデータ312などをさらに格納したセキュアコンテンツ842を作成し、セキュアコンテンツ842をユーザホームネットワーク303に配給する。

【0533】ユーザホームネットワーク303では、オンラインの場合にはCモジュール311を介してセキュアコンテンツ842がSAM305₁などに提供され、SAM305₁などにおいて、キープファイルKFに格納されたコンテンツ鍵データK_cおよび権利書データ106などが配信用鍵データKD₁～KD_nなどを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテンツ832が配給される場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

【0534】なお、ユーザホームネットワーク303、303aにおけるセキュアコンテンツ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。また、図139に示す例では、コンテンツプロバイダ301から共通データベース840、共通データベース840からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキープファイルKFを格納したセキュアコンテンツを送る場合（インバンドの場合）を例示したが、コンテンツファイルCFおよびキープファイルKFを同一経路で別々に送

信してもよい(アウト・オブ・バンドの場合)。また、図140に示すように、コンテンツプロバイダ301から共通データベース830にコンテンツファイルCFを格納し、サービスプロバイダ310が共通データベース820からコンテンツファイルCFを得ると共に、EMDサービスセンタ302からサービスプロバイダ310にキーファイルKFを送るようにもよい。このとき、サービスプロバイダ310が得たコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からサービスプロバイダ310にキーファイルKFが送られる。

【0535】サービスプロバイダ310は、共通データベース840から得たコンテンツファイルCFと、EMDサービスセンタ302から得たキーファイルKFと、ブライスタグデータ312とを格納してセキュアコンテンツ842を作成する。共通データベース830は、複数のコンテンツプロバイダ301が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

【0536】また、図141に示すように、EMDサービスセンタ302が作成したキーファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにもよい。このときも、SAM305₁、305₁₂などに提供されたコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からSAM305₁、305₁₂などにキーファイルKFが送られる。また、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。ブライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよいし、EMDサービスセンタ302がユーザホームネットワーク303、303aに配給してもよい。

【0537】第8実施形態

図142は、本発明の第8実施形態のEMDシステムを説明するための図である。本実施形態のEMDシステムでは、例えば、コンテンツプロバイダ301からEMDサービスセンタ302に提供されたマスタソースを用いてEMDサービスセンタ302が作成した図5(A)に示すコンテンツファイルCF、あるいはコンテンツプロバイダ301が作成してEMDサービスセンタ302に提供した図5(A)に示すコンテンツファイルCFと、EMDサービスセンタ302が作成した図5(B)に示すキーファイルKFとが、EMDサービスセンタ302によってサービスプロバイダ310を介して、あるいは直接的にユーザホームネットワーク303のSAM305₁に配給される。ここで、サービスプロバイダ310は、コンテンツファイルCFの販売価格を示すブライスタグデータ312をユーザホームネットワーク303に

送ると共に、ブライスタグデータ312をEMDサービスセンタ302に登録して格納化する。また、サービスプロバイダ310は、自らを、配信事業者としてEMDサービスセンタ302に登録する。

【0538】本実施形態のEMDシステムでは、ユーザホームネットワーク303の例えばSAM305₁が、サービスプロバイダ310あるいはEMDサービスセンタ302から得たコンテンツファイルCFおよびキーファイルKFを、ユーザホームネットワーク303内のSAM305₂および/またはユーザホームネットワーク303a内のSAM305₁₂などに配信する配信事業者となる。但し、この場合に、例えば、EMDサービスセンタ302は、SAM305₁がコンテンツファイルCFに格納されたコンテンツデータCを購入した後に、当該購入したコンテンツデータCを、何らかの販売マージンを加えて販売(再配付)して利益を上げることが禁止する。本実施形態のEMDシステムでは、購入形態が未決定のコンテンツデータC、あるいは、購入形態として再生課金が決定されているコンテンツデータCを、販売利益マージンをとらずに再配付することを条件に、SAM305₁がコンテンツデータCを他のSAMに複製することを許可する。なお、これを機器間再配布と呼ぶ。また、本実施形態のEMDシステムでは、SAM305₁がサービスプロバイダ310から配給を受けたコンテンツファイルCF(あるいはセキュアコンテンツ)に関しては、販売利益マージンをとらない形態での機器間売買は許可される。また、本実施形態では、SAM305₁が、販売利益マージンをとる形態でのコンテンツデータCの販売(配付)を行う場合には、SAM305₁はEMDサービスセンタ302に自らを配信事業者として登録して許諾を受けると共に、コンテンツデータCの販売価格を示すブライスタグデータ312をEMDサービスセンタ302に登録する。そして、SAM305₁は、サービスプロバイダ310を介さずに、EMDサービスセンタ302内のCFデータベース802aおよびKFデータベース153aから直接的にコンテンツファイルCFおよびキーファイルKFの配給を受ける。

【0539】第9実施形態

図143は、本発明の第9実施形態のEMDシステムを説明するための図である。本実施形態のEMDシステムでは、コンテンツプロバイダ301のそれぞれが、コンテンツプロバイダとしての役割に加えて、EMDサービスセンタ302としての役割を果たすことを特徴とする。おの場合に、複数のコンテンツプロバイダ301がある場合に、それぞれのコンテンツプロバイダ301は、それぞれのEMDサービスセンタ302としての役割を持つ。コンテンツプロバイダ301は、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテンツ851をサービスプロバイダ310に配給する。サービスプロバイダ310は、セキュアコンテンツ8

183

51が格納したコンテンツファイルCF、キーファイルKFに、さらにブライスクデータ312を加えてセキュアコンテンツ852を作成し、これをユーザホームネットワーク303に転送する。ユーザホームネットワーク303、303aでは、キーファイルKF内に格納された権利データ106に基づいてコンテンツファイルCFの購入形態などを決定し、それに応じた利用履歴データ308を作成し、これをコンテンツプロバイダ301内のEMDサービスセンタ302に送信する。このとき、利用履歴データ308は、コンテンツプロバイダ301毎に作成される。コンテンツプロバイダ301のEMDサービスセンタ302は、利用履歴データ308に基づいて、SAM3051、3051aのユーザが支払った利益を、自らと対応するサービスプロバイダ310との間で分配する。また、ユーザホームネットワーク303のCAモジュール311から、配信サービスに関するの履歴データが対応するサービスプロバイダ310に送られ、サービスプロバイダ310において配信サービスに対しての課金処理が行われる。

【0540】本発明は上述した実施形態には限定されない。上述した実施形態では、コンテンツデータとしてオーディオデータを用いる場合を例示したが、コンテンツデータとして、ビデオデータ、オーディオ・ビデオデータ、テキストデータおよびコンピュータプログラムなどを用いてもよい。また、上述した実施形態では、EMDサービスセンタ102、302において、キーファイルKFを作成する場合を例示したが、コンテンツプロバイダ101、301においてキーファイルKFを作成することも可能である。この場合に、図7に対応するキーファイルKFのフォーマットは、図144に示すようになる。図144に示すように、当該キーファイルKFは、コンテンツプロバイダ101、301の秘密鍵データKCPsを用いて作成された署名データが用いられる点を除いて、図7に示すキーファイルKFと基本的に同じ情報を有している。

【0541】また、上述した実施形態では、ユーザホームネットワーク103、303からEMDサービスセンタ102、302に、利用制御状態データ166をリアルタイムで送信する場合を例示したが、利用制御状態データ166をコンテンツプロバイダ101、301および/またはサービスプロバイダ310に送信するようにしてもよい。これにより、コンテンツプロバイダ101、301およびサービスプロバイダ310は、自らが提供および配給したコンテンツの購入状況を照会に把握でき、その後のサービスに反映できる。

【0542】以下、上述した本実施形態のEMDシステムによる効果を、従来技術およびその問題点を述べながら再び説明する。デジタル放送（データ放送）、インターネットなどのデジタルネットワークが発達していない時代に、デジタルコンテンツ（コンテンツデータ）を流

184

用させる手段として使用されていたROM型記録媒体では、デジタルコンテンツを非暗号化の状態で記録して流通させていた。デジタルネットワークが発達していない時代では、これらのコンテンツの著作権保護をおこなうのは、ユーザホームネットワーク上でユーザによるカジュアルコピーを防ぐ方法を考えるだけで良かった。

【0543】しかしながら、デジタルネットワークが発達してきた昨今では、非暗号化コンテンツが搭載されているROM型記録媒体を一般市民が、いつ、どこでも、自由に入手することができるために、各自がこれらを購入し、圧縮してネットワークにアップロードすることが簡単にできてしまう。特にインターネットは世界中につながっているネットワークなので、非暗号化コンテンツを無料でインターネット上にアップロードし、市民はそれを無料で自分の個人端末にダウンロードすることが可能となってしまう。コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害する可能性が出てきている。

【0544】また、非暗号化の状態ではアップロードせず、自らが、そのコンテンツに対し、独自方式の電子透かし情報を含め込み、暗号化をおこなうことで独自方式の課金機能を備え、インターネット上で著作権の許可なしに、目の届かないところで勝手に、デジタルコンテンツの販売をおこなうことも可能となっている。このときは、売り上げの一部がコンテンツの権利者に還元されないで、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害することになる。また、著作権者の許諾を得て、売り上げの一部をコンテンツの権利者（コンテンツプロバイダ）に還元する契約を権利者側と事前におこなうことで、これらのデジタルコンテンツを配信して利益が得られる配信サービスをおこなうことが可能になるが、基本的にコンテンツプロバイダは、こういったコンテンツの2次利用による流通体系をあまり好ましく思っていない。コンテンツの2次利用によるビジネスとは、たとえばレンタルビジネス、中古販売などが相当する。2次利用による配信サービスが盛況する時は、必ず著作権侵害の問題が起こり、サービス自体を軌道に載せるまで時間がかかる。コンテンツプロバイダと事前契約をおこなうことなく、まず配信サービスを始めてしまい、著作権侵害という問題になってから、権利者側への利益配分なり著作権保護が考慮され配信サービスとしての許諾が得られる。レンタルC、レンタルビデオが相当する。ゲームソフトの中古販売などは深刻な問題である。現在ゲームソフトの中古販売ビジネスでは、売り上げの利益の一部がコンテンツの権利者側に還元されないで、権利者側は裁判で告訴しているが却下され、権利者側にとって非常に酷になっている。新作ソフトの半額以下で大量に販売されるので、ユーザからして魅力がある市場で、新作ソフトの売り上げにも影響を及ぼす。

185

【0545】コンテンツの2次利用というのは、本来コンテンツの権利者がROM型記録媒体を流通手段とし、そのデジタルコンテンツ記録済のROM型記録媒体を商品として流通させて利益を得ている訳で、それらを購入したユーザによって、その商品をさらに流通させることで、購入したユーザが利益を得ることは、たとえ利益の一部が還元されたとしても、(コンテンツプロバイダ)権利者側の立場からするとあまり好ましく思わない。映画コンテンツなどは、録音権/録画権というものがコンテンツの権利者側に法律で保障されており、権利者が世に流通させたコンテンツを、それを購入した時点で、その購入ユーザの手元からは流通しないことを前提としている。ゲームソフトの権利者団体は、この頒布権の権利をゲームソフトにも利用し、2次利用ビジネスの抑制を裁判で訴えている。

【0546】コンテンツの権利者は、自分が著作権を持っているデジタルコンテンツについては、それを流用させる流通業者を管理下におきたい(誰に流通させているか、を知っておきたい)。自分が著作権を持っているデジタルコンテンツを流通させて配信サービスをおこない利益を得ることを希望している配信事業者がいる場合は、コンテンツの権利者から直接デジタルコンテンツを渡せるようなシステムが望ましい。なお、ここで述べている流通業者とは、デジタルコンテンツの対価に、さらに何%かの利益マージンを徴収することで利益を得る業者を指す。デジタルコンテンツを他機器/記録媒体へ渡すときに利益マージンを徴収する場合、そのコンテンツ先買セッション配信サービスとして定義し、利益マージンを徴収しない場合を機器間再配付として定義し、これは超流通の原理により合法である。コンテンツプロバイダが流通させた非暗号化コンテンツが記録されているROM型記録媒体からサービスプロバイダが、自分の配信サービス用コンテンツをオーサリングし、配信サービスをおこなう現状のデジタルコンテンツのネットワーク流通管理システムにおいて、コンテンツプロバイダが所有している一つのデジタルコンテンツが複数のサービスプロバイダによって配信される状況を考えると、同一コンテンツであるにも関わらず、各々のサービスプロバイダが採用するCAモジュール/電子決済ツールにて権利処理がおこなわれるようにオーサリングされるため、使用される暗号鍵(コンテンツ鍵データ)、コンテンツの使用許諾条件(権利者データ)のフォーマットが各サービスプロバイダによって各々異なり、ユーザホームネットワーク上で共通の権利処理ルールを提供することができない。こういった場合は、CAモジュール/電子決済ツールで利用する鍵データ類をすべてネットワーク機器のCAモジュール/電子決済ツールで消算し、あとはSCMSのルールに準拠することでユーザホームネットワーク上での共通の権利処理ルールを実現している。また、CAモジュール/電子決済ツールの鍵で暗号化さ

186

れたコンテンツと鍵データを、そのままネットワーク機器を通過してユーザホームネットワークバス(IEEE1394など)を經由してストレージ機器の記録媒体に記録し、1394バス上につながる機器から随時的にネットワーク機器を経由してコンテンツの購入、決済処理ができたとしても、暗号化コンテンツを復号するためのデスクトップがネットワーク機器に存在するので、結局再生時にネットワーク機器まで、コンテンツと鍵データを戻さないで再生できない(ネットワークCA)。

【0547】上述したように、現在までに世の中に広く流通している非暗号化コンテンツが記録されているROM型記録媒体の存在が、現状のデジタルコンテンツネットワーク配信サービスにとって問題の根源となっている。デジタルコンテンツのコンテンツ形態が、コンテンツプロバイダ以外の第3者によって作成される可能性を誇っており、さらに、ユーザに対して、そのコンテンツを販売した人が、その対価を入手するシステムであるため、コンテンツの2次利用などコンテンツプロバイダの利益が不当に損なわれる可能性がある。また、オーサリングしたデジタルコンテンツの流通管理をコンテンツプロバイダが厳密におこなっていないため、自分が著作権を持っているデジタルコンテンツが複製出す金利益、およびそこから自分の利益分が還元されているかどうかを監視することが難しい。

【0548】前述した本実施形態のEMDシステムは、上述したような従来の問題を解決した。すなわち、本実施形態のEMDシステムでは、コンテンツプロバイダがオーサリングしたデジタルコンテンツは、すべてコンテンツプロバイダ側で、コンテンツ形態や権利者データを作成し、コンテンツプロバイダ側のデータベースに管理しておく。コンテンツの権利者データに関しては、さらに第3の信頼機関であるFMDサービスセンタ(クリアリングハウス)で權威化し登録しておく。こうすることで、コンテンツプロバイダの關係者が、デジタルコンテンツの権利処理ルールを完全に自分の管理下におくことができ、流通経路をコンテンツプロバイダ側で管理することを可能とする。また、本件では、このコンテンツプロバイダ側で作成した権利者のデータの内容を、ユーザとの間に存在する流通業者が見ることができないような仕掛けを提供する。また、本実施形態のEMDシステムでは、ROM型記録媒体を、ひとつの流通手段として考えて、そこに搭載するデジタルコンテンツの存在をROM型記録媒体から遊離させる。流通手段、流通経路によらず、デジタルコンテンツ単体で、その存在価値を表現するコンテンツ形態を提案する。デジタルコンテンツはコンテンツプロバイダ側である規定の形式で管理されるので、ROM型記録媒体に、その形式のデジタルコンテンツを搭載すると考えることで、デジタル記録媒体で流通されようが、デジタルネットワークで流通されようが、ユーザホームネットワーク上では、ROM→RAM、ネ

187

ットワーク→RAMにおいて共通の権利処理ルールを提供することが可能となる。デジタルコンテンツの販売セッションを、すべてコンテンツプロバイダが規定、管理する形式でおこなう。これにより、流通手段、流通経路によらない共通の権利処理が可能となる。また、このコンテンツプロバイダ側で規定されたコンテンツ形態は、デジタルコンテンツの売買をおこなう上での最小単位と定済することで、その後の流通過程で利用されるコンテンツ形態の種類に依存せず共通の権利処理ルールを提供することができる。ユーザホームネットワークで購入したときに生成される課金情報を、サービスプロバイダに返すのではなく、第3の信頼機関であるEMDサービスセンタに返し、そこからサービスプロバイダに返すことによりコンテンツの2次利用によるビジネスの問題点を解決した。

【0549】

【発明の効果】以上説明したように、本発明によれば、データ提供装置が提供したコンテンツデータのデータ処理装置における取り扱いを、データ提供装置による権利管理データに基づいて行わせることが可能になる。その結果、データ提供装置の関係者によるコンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図1】図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】図2は、本発明のセキュアコンテナの概念を説明するための図である。

【図3】図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図である。

【図4】図4は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図5】図5は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図6】図6は、図5に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図7】図7は、図5に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図8】図8は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図9】図9は、コンテンツIDを説明するための図である。

【図10】図10は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図11】図11は、セキュアコンテナのハイパーリン

188

ク構造を説明するための図である。

【図12】図12は、本実施形態で用いられるROM型の記録媒体の第1の例を説明するための図である。

【図13】図13は、本実施形態で用いられるROM型の記録媒体の第2の例を説明するための図である。

【図14】図14は、本実施形態で用いられるROM型の記録媒体の第3の例を説明するための図である。

【図15】図15は、本実施形態で用いられるRAM型の記録媒体の第1の例を説明するための図である。

【図16】図16は、本実施形態で用いられるRAM型の記録媒体の第2の例を説明するための図である。

【図17】図17は、本実施形態で用いられるRAM型の記録媒体の第3の例を説明するための図である。

【図18】図18は、コンテンツプロバイダからEMDサービスセンタに送信される登録要求用ソフトウェアを説明するための図である。

【図19】図19は、コンテンツプロバイダからEMDサービスセンタへの登録処理の手順を示すフローチャートである。

【図20】図20は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図21】図21は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図22】図22は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図23】図23は、図1に示すEMDサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図24】図24は、図1に示すEMDサービスセンタの機能ブロック図であり、SAMおよび図1に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図25】図25は、図1に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図26】図26は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図27】図27は、図25に示す外部メモリに記憶されるデータを説明するための図である。

【図28】図28は、スタックメモリに記憶されるデータを説明するための図である。

【図29】図29は、図1に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図30】図30は、図26に示す記憶部に記憶されるデータを説明するための図である。

【図31】図31は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れ

を示す図である。

【図 32】図 32 は、図 25 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入力形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAM内での処理の流れを説明するための図である。

【図 33】図 33 は、図 32 に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図 34】図 34 は、購入形態が決定したセキュアコンテンツのフォーマットを説明するための図である。

【図 35】図 35 は、図 32 に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図 36】図 36 は、コンテンツの購入形態が未決定の図 7 に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理の流れを説明するための図である。

【図 37】図 37 は、図 36 に示す場合において、SAM内でのデータの流れを示す図である。

【図 38】図 38 は、ユーザホームネットワーク内のAV機器において購入形態が未決定のROM型の記録媒体からセキュアコンテンツを読み出して、これを他のAV機器に転送してRAM型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 39】図 39 は、図 38 に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図 40】図 40 は、図 38 において、転送元のSAMから転送先のSAMに転送されるセキュアコンテンツのフォーマットを説明するための図である。

【図 41】図 41 は、図 38 に示す場合における転送先のSAM内でのデータの流れを示す図である。

【図 42】図 42 は、図 1 に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 43】図 43 は、図 1 に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 44】図 44 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図 45】図 45 は、SAMが作成するSAM登録リストのデータフォーマットを説明するための図である。

【図 46】図 46 は、EMDサービスセンタが作成するSAM登録リストのデータフォーマットを説明するた

めの図である。

【図 47】図 47 は、図 1 に示すコンテンツプロバイダの全体動作のフローチャートである。

【図 48】図 48 は、第 1 実施形態の EMD システムにおいて用いられるセキュアコンテンツの配送プロトコルの一例を説明するための図である。

【図 49】図 49 は、本発明の第 1 実施形態の第 2 変形例を説明するための図である。

【図 50】図 50 は、本発明の第 1 実施形態の第 3 変形例を説明するための図である。

【図 51】図 51 は、本発明の第 1 実施形態の第 4 変形例において第 1 の手法を採用した場合を説明するための図である。

【図 52】図 52 は、本発明の第 1 実施形態の第 4 変形例において第 2 の手法を採用した場合を説明するための図である。

【図 53】図 53 は、本発明の第 1 実施形態の第 5 変形例を説明するための図である。

【図 54】図 54 は、本発明の第 1 実施形態の第 6 変形例の第 1 のパターンを説明するための図である。

【図 55】図 55 は、本発明の第 1 実施形態の第 6 変形例の第 2 のパターンを説明するための図である。

【図 56】図 56 は、本発明の第 1 実施形態の第 6 変形例の第 3 のパターンを説明するための図である。

【図 57】図 57 は、本発明の第 1 実施形態の第 6 変形例の第 4 のパターンを説明するための図である。

【図 58】図 58 は、本発明の第 1 実施形態の第 6 変形例の第 5 のパターンを説明するための図である。

【図 59】図 59 は、本発明の第 2 実施形態の EMD システムの全体構成図である。

【図 60】図 60 は、図 59 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテンツに関するデータの流れを示す図である。

【図 61】図 61 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートである。

【図 62】図 62 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートである。

【図 63】図 63 は、図 59 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図 64】図 64 は、サービスプロバイダにおいて行われるセキュアコンテンツの作成処理の手順を示すフローチャートである。

【図 65】図 65 は、図 59 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテンツのフォーマットを説明するための図である。

【図 66】図 66 は、図 65 に示すセキュアコンテンツに

191

格納されたコンテンツファイルの送信形態を説明するための図である。

【図 67】図 67 は、図 65 に示すセキュアコンテナに格納されたキープファイルの送信形態を説明するための図である。

【図 68】図 68 は、図 59 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図である。

【図 69】図 69 は、サービスプロバイダから EMD サービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図 70】図 70 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 71】図 71 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 72】図 72 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、SAM との間で送受信されるデータに関連するデータの流れを示す図である。

【図 73】図 73 は、利用履歴データの内容を説明するための図である。

【図 74】図 74 は、図 59 に示すネットワーク機器の構成図である。

【図 75】図 75 は、図 74 に示す CA モジュールの機能ブロック図である。

【図 76】図 76 は、図 74 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図 77】図 77 は、図 76 に示す記憶部に記憶されるデータを説明するための図である。

【図 78】図 78 は、図 74 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図 79】図 79 は、SAM におけるセキュアコンテナの購入形態の決定処理の手順を示すフローチャートである。

【図 80】図 80 は、購入形態が決定された後のキープファイルのフォーマットを説明するための図である。

【図 81】図 81 は、図 74 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送先の SAM 内での処理の流れを説明するための図である。

【図 82】図 82 は、図 81 に示す場合の転送元の SAM 内でのデータの流れを示す図である。

【図 83】図 83 は、図 81 に示す場合の転送先の SAM 内でのデータの流れを示す図である。

192

【図 84】図 84 は、図 59 に示す EMD システムの全体動作のフローチャートである。

【図 85】図 85 は、図 59 に示す EMD システムの全体動作のフローチャートである。

【図 86】図 86 は、第 2 実施形態の EMD システムにおけるサービスプロバイダからユーザホームネットワークへのセキュアコンテナの配付形態の一例を説明するための図である。

【図 87】図 87 は、第 2 実施形態の EMD システムが採用するセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図 88】図 88 は、図 87 においてユーザホームネットワークからサービスプロバイダ 310 へのセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 89】図 89 は、図 87 においてコンテンツプロバイダから EMD サービスセンタへのキープファイルなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 90】図 90 は、図 87 においてサービスプロバイダから EMD サービスセンタへのプライスタグデータ 312 などを配送する際に用いられる配送プロトコルを説明するための図である。

【図 91】図 91 は、図 87 においてユーザホームネットワーク内でセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 92】図 92 は、デジタル放送のデータ放送方式に XML/SMIL/BML を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 93】図 93 は、デジタル放送のデータ放送方式に MHPEG を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 94】図 94 は、インターフェイスのデータ放送方式に XML/SMIL を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 95】図 95 は、ユーザホームネットワークから EMD サービスセンタに利用履歴データなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 96】図 96 は、ユーザホームネットワーク内においてセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 97】図 97 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システムの構成図である。

【図 98】図 98 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD

193

システムの構成図である。

【図 99】図 99 は、本発明の第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

【図 100】図 100 は、本発明の第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

【図 101】図 101 は、公開鍵証明書データの取得ルート形態を説明するための図である。

【図 102】図 102 は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 103】図 103 は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 104】図 104 は、SAM の公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 105】図 105 は、SAM の公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図 106】図 106 は、図 47 に示す EMD システムにおいて、EMD サービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図 107】図 107 は、図 106 に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体の EMD サービスセンタ内に設けた場合の EMD システムの構成図である。

【図 108】図 108 は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 109】図 109 は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 110】図 110 は、コンテンツプロバイダが権利管理用クリアリングハウスおよび電子決済用クリアリングハウスの双方の機能をさらに備えている場合の EMD システムの構成図である。

【図 111】図 111 は、本発明の第 2 実施形態の第 8 変形例において、図 47 に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテンツのフォーマットを説明するための図である。

【図 112】図 112 は、図 111 に示すコンテンツファイルとキーファイルとの間のディレクトリ構造データによるリンク関係を説明するための図である。

【図 113】図 113 は、コンテンツファイルとキーファイルとの間のディレクトリ構造のその他の例を説明するための図である。

【図 114】図 114 は、本発明の第 2 実施形態の第 8 変形例において、図 47 に示すサービスプロバイダから SAM に提供されるセキュアコンテンツのフォーマットを説明するための図である。

194

【図 115】図 115 は、コンボジット型のセキュアコンテンツのデータフォーマットの第 1 の概念を説明するための図である。

【図 116】図 116 は、コンボジット型のセキュアコンテンツのデータフォーマットの第 2 の概念を説明するための図である。

【図 117】図 117 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 1 の手法を採用した場合を説明するための図である。

【図 118】図 118 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 2 の手法を採用した場合を説明するための図である。

【図 119】図 119 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいてファイル形式を採用しない場合のデータフォーマットを説明するための図である。

【図 120】図 120 は、本発明の第 2 実施形態の第 10 変形例に係わる EMD システムの構成図である。

【図 121】図 121 は、本発明の第 2 実施形態の第 11 変形例の第 1 のパターンに係わる EMD システムの構成図である。

【図 122】図 122 は、本発明の第 2 実施形態の第 11 変形例の第 2 のパターンに係わる EMD システムの構成図である。

【図 123】図 123 は、本発明の第 2 実施形態の第 11 変形例の第 3 のパターンに係わる EMD システムの構成図である。

【図 124】図 124 は、本発明の第 2 実施形態の第 11 変形例の第 4 のパターンに係わる EMD システムの構成図である。

【図 125】図 125 は、本発明の第 2 実施形態の第 11 変形例の第 5 のパターンに係わる EMD システムの構成図である。

【図 126】図 126 は、本発明の第 2 実施形態の第 9 変形例に係わる EMD システムの構成図である。

【図 127】図 127 は、本発明の第 2 実施形態におけるセキュアコンテンツのファイル包括大小関係を説明するための図である。

【図 128】図 128 は、本発明の第 3 実施形態の EMD システムを説明するための図である。

【図 129】図 129 は、図 128 に示す EMD サービスセンタの機能ブロック図である。

【図 130】図 130 は、本発明の第 3 実施形態の EMD システムの変形例を説明するための図である。

【図 131】図 131 は本発明の第 4 実施形態の EMD システムを説明するための図である。

【図 132】図 132 は本発明の第 4 実施形態の EMD システムの変形例を説明するための図である。

【図 133】図 133 は本発明の第 5 実施形態の EMD システムを説明するための図である。

【図134】図134は本発明の第5実施形態のEMDシステムの変形例を説明するための図である。

【図135】図135は本発明の第5実施形態のEMDシステムのその他の変形例を説明するための図である。

【図136】図136は本発明の第6実施形態のEMDシステムを説明するための図である。

【図137】図137は本発明の第6実施形態のEMDシステムの変形例を説明するための図である。

【図138】図138は本発明の第6実施形態のEMDシステムのその他の変形例を説明するための図である。

【図139】図139は本発明の第7実施形態のEMDシステムを説明するための図である。

【図140】図140は本発明の第7実施形態のEMDシステムの変形例を説明するための図である。

【図141】図141は本発明の第7実施形態のEMDシステムのその他の変形例を説明するための図である。

【図142】図142は本発明の第8実施形態のEMDシステムを説明するための図である。

【図143】図143は本発明の第9実施形態のEMDシステムを説明するための図である。

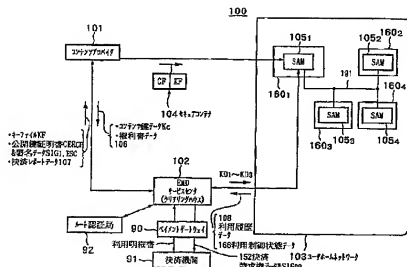
【図144】図144は、コンテンツプロバイダにおいてキーファイルを作成した場合のキーファイルのフォーマットを説明するための図である。

【図145】図145は、従来のEMDシステムの構成図である。

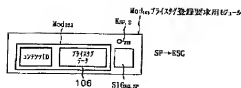
【符号の説明】

90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100、300…EMDシステム、101、301…コンテンツプロバイダ、102、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、1051…1054、3051…3054…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、1601…ネットワーク機器、1602…1604…AV機器、152、152c、152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【図1】



【図69】



【図27】

外部に2012記憶されるデータ

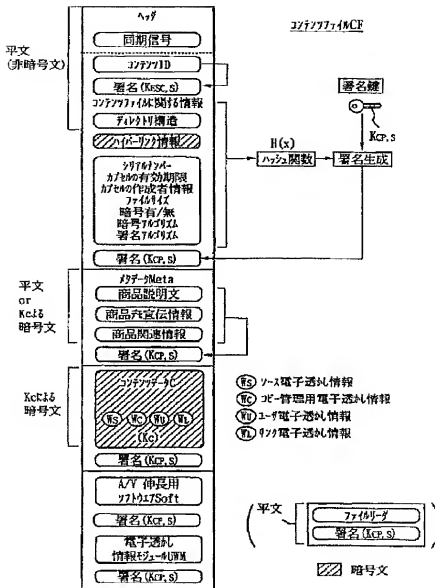
利用履歴データ108
SAM登録リスト

【図73】

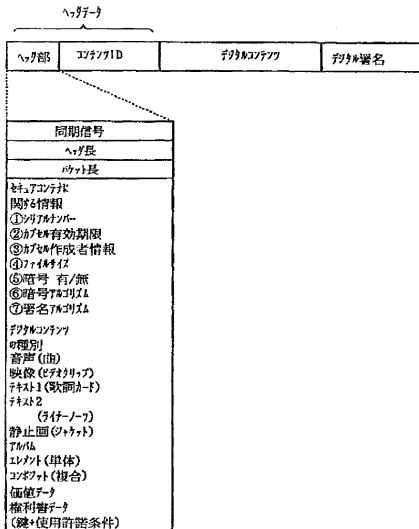
利用履歴データ308の内容

識別子Content_ID
識別子CP_ID
識別子SP_ID
コンテンツデータの番号諸元データ
コンテンツデータの圧縮方法
記録媒体の識別子Media_ID
識別子SAM_ID、
ユーザのUSER_ID

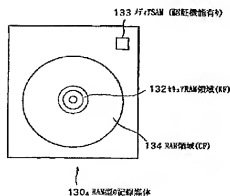
【図6】



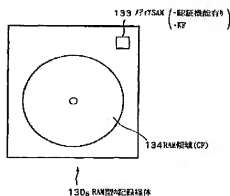
【図8】



【図15】

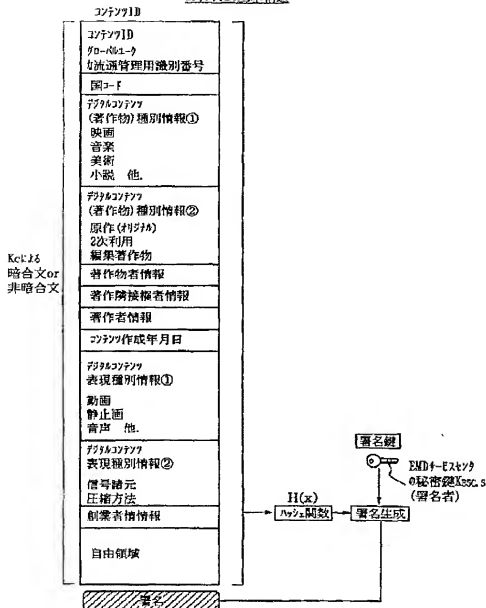


【図16】

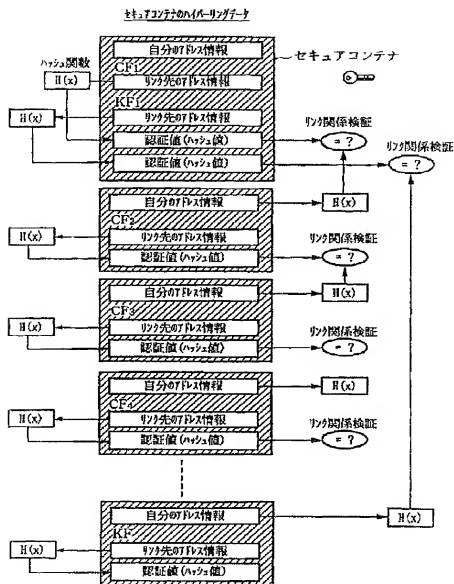


【図9】

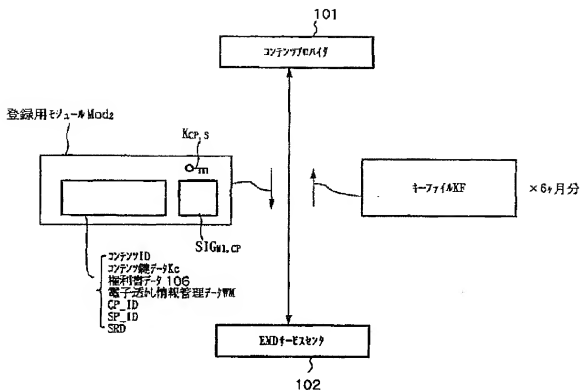
コンテンツIDの基本構造



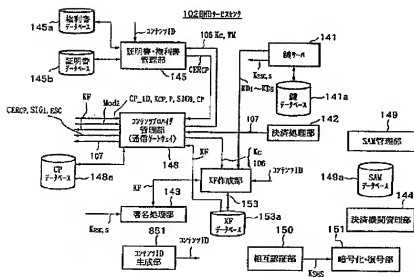
【図 11】



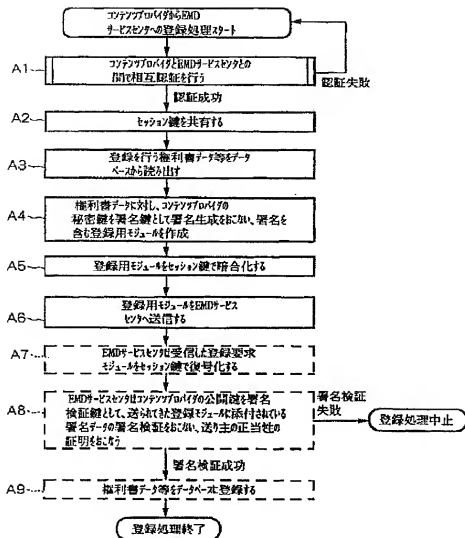
【図 18】



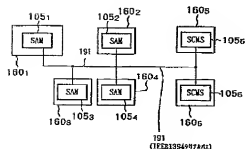
【図 23】



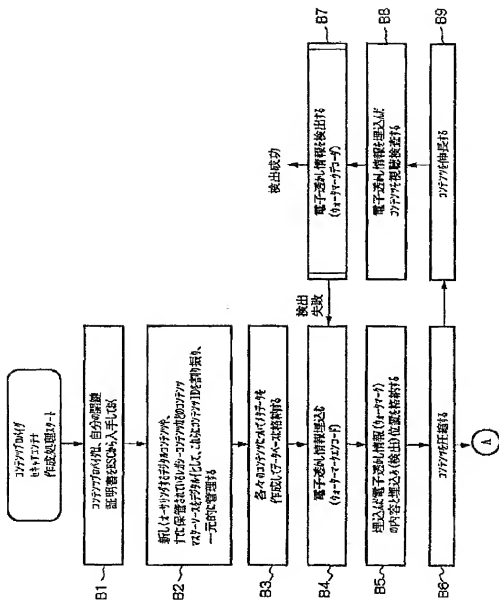
【图 19】



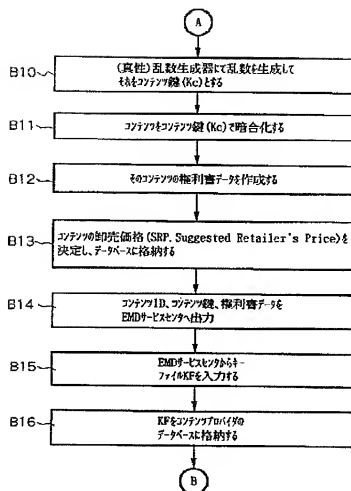
【圖 4-4】



【図20】



【図21】



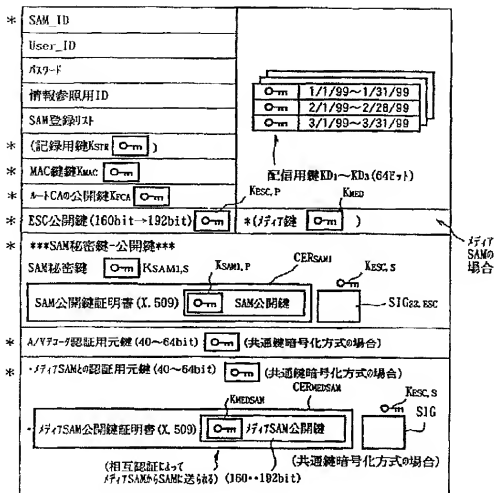
[illegible]

The block diagram illustrates a video recording system architecture. At the top, a "ビデオデッキ101" (Video Deck 101) connects via a "104" interface to a "通信CPU-8" (Communication CPU-8) labeled 162. Below this, a central "SAM" (System Area Module) block 105₁ is connected to several components: a "個人・利用形態操作部" (Personal/User Type Operation Section) 165, which also interfaces with a "BIO" (Biometric Input Output) unit; a "外部FIFO (フリップフロップ)" (External FIFO (Flip-Flop)) 201; and a "再生CPU-9" (Playback CPU-9) 160 at the bottom. To the right of the SAM, there are two modules: "ビデオSAM 107" (Video SAM 107) and "ビデオ-FIFO 104" (Video FIFO 104). The SAM 105₁ is further connected to a large functional block 163, which contains internal modules: "復号部(De)" (Decoding Section) 221, "変調部(En)" (Modulation Section) 222, "相互接続部" (Interconnection Section) 220, "制御部" (Control Section) 223, "半導体メモリ" (Semiconductor Memory) 225, and "電子選択情報記憶部" (Electronic Selection Information Storage Section) 224. Data flow is indicated by arrows labeled with codes such as "k", "c", "f", "g", and "h". A common output line "C" exits from the bottom of block 163.

The diagram shows a central SAM (Signal Analysis Module) block. Above it is a '受信機 (104)' (Receiver 104) which receives '電波 (104)' (Radio waves 104). Below the SAM is a '送信機 (105)' (Transmitter 105). To the left of the SAM is a 'CPU' block connected to a '利用メモリ (RAM)' (Used Memory) and a 'ROM'. To the right is a '外部メモリ (106)' (External Memory). Below the SAM is a '外部FEV' (External FEV) block. The SAM is connected to a '信号処理部 (103)' (Signal Processing Unit 103). Inside this unit are several sub-blocks: '信号部 (101)' (Signal Unit 101) containing '信号部 (Fm)' (Signal Unit Fm) and '信号部 (D)' (Signal Unit D); '相互接続部 (102)' (Interconnection Unit 102); '制御部 (103)' (Control Unit 103); '平衡検出回路 (104)' (Balance Detection Circuit 104); and '電子線偏光検出回路 (105)' (Electron Beam Polarization Detection Circuit 105). Various signal lines (101, 102, 103, 104, 105) connect these sub-blocks and the SAM to the external FEV and memory blocks.

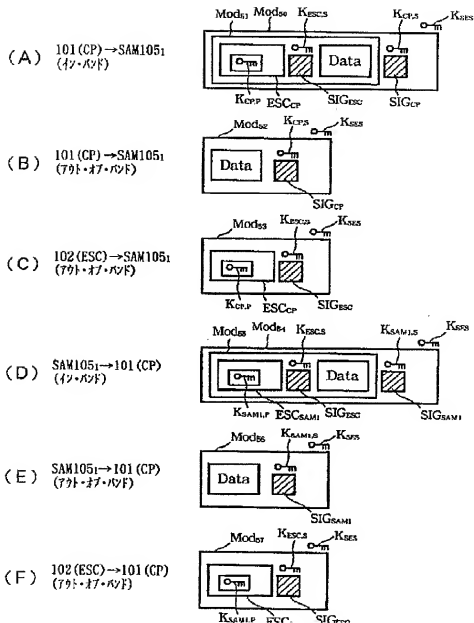
【図 30】

記憶部192に記憶されるデータ



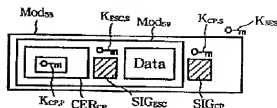
[illegible]

【図 4 2】

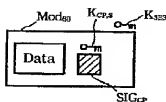


【図 43】

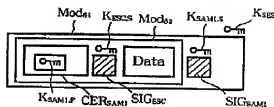
(G) 101 (CP) → 102 (ESC)
(イソ・バツフ)



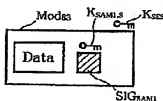
(H) 101 (CP) → 102 (ESC)
(79ト・バツ・バツフ)



(I) SAM1051 → 102 (ESC)
(イソ・バツフ)

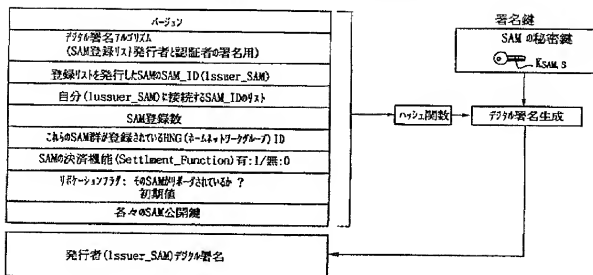


(J) SAM1051 → 102 (ESC)
(79ト・バツ・バツフ)



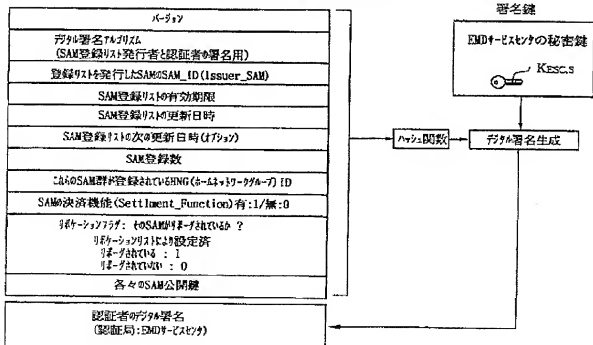
【図 4 5】

SAM登録リスト (SAM Registration List) (SAM作成)

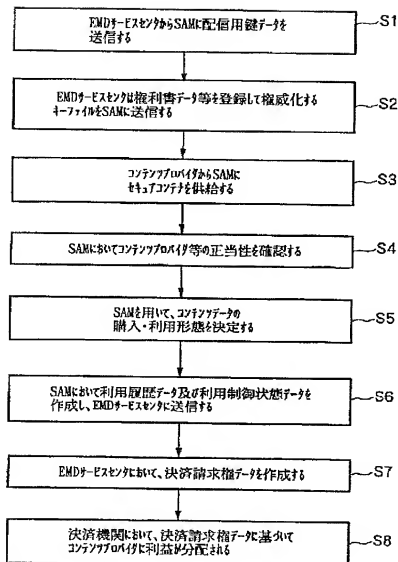


【図 4 6】

SAM登録リスト (EMDサビセンタ作成)

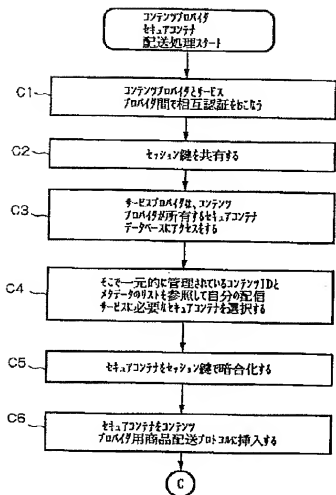


【図 47】

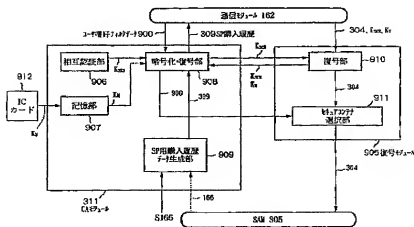


[illegible]

【图 6-1】



【例 7 5】



```

graph TD
    C((C)) --> C7[C7: サービスプロバイダがダウンロードを行う]
    C7 --> C8[C8: コンテンツプロバイダ用商品配送プロトコルからセッションIDを取り出す]
    C8 --> C9[C9: セッションIDをセッション鍵で復号する]
    C9 --> C10[C10: セッション署名検証をともに行(送り主の正当性)]
    C10 -- "署名検証失敗" --> End1([受取り中止])
    C10 -- "署名検証成功" --> C11[C11: サービスプロバイダが所有するセッションデータベースへ格納する]
    C11 --> End2([終了])
  
```

Figure 10 is a flowchart illustrating the signature verification process. It begins with a start node 'C'. The process follows these steps:

- C7:** サービスプロバイダがダウンロードを行う (Service provider performs download).
- C8:** コンテンツプロバイダ用商品配送プロトコルからセッションIDを取り出す (Extract session ID from content provider's product delivery protocol).
- C9:** セッションIDをセッション鍵で復号する (Decrypt session ID with session key).
- C10:** セッション署名検証をともに行(送り主の正当性) (Perform session signature verification together (sender's legitimacy)).

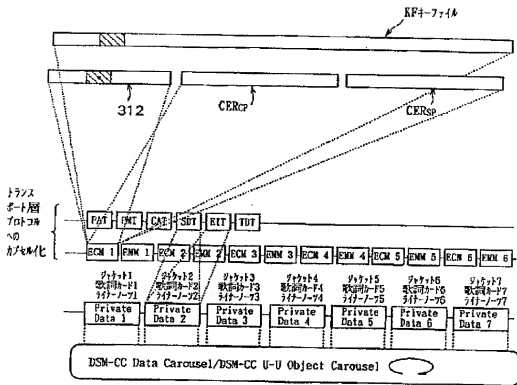
From step C10, the process branches based on the verification result:

- If the signature verification fails (署名検証失敗), the process ends at **受取り中止** (Acceptance stopped).
- If the signature verification is successful (署名検証成功), the process continues to **C11:** サービスプロバイダが所有するセッションデータベースへ格納する (Store in session database owned by service provider).

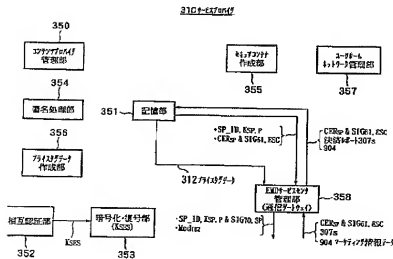
The process concludes at the **終了** (End) node.

[illegible]

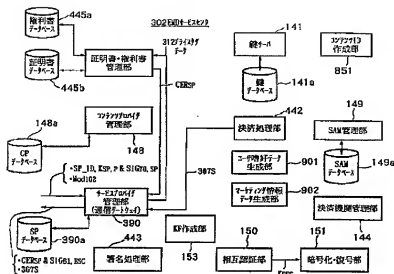
【圖 6 7】



【图 6 8】



【図70】



【図71】

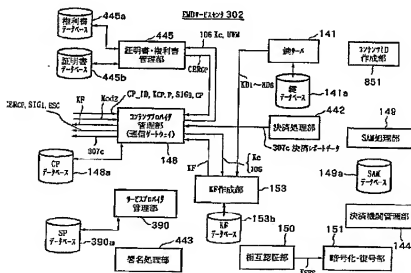
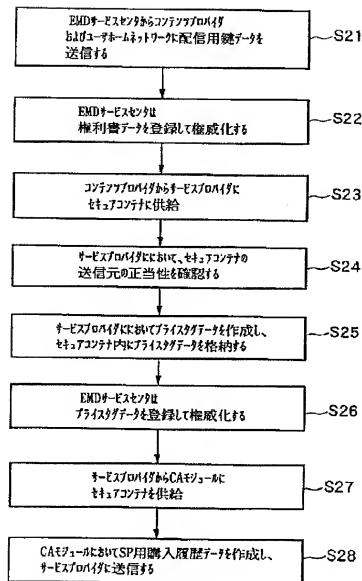


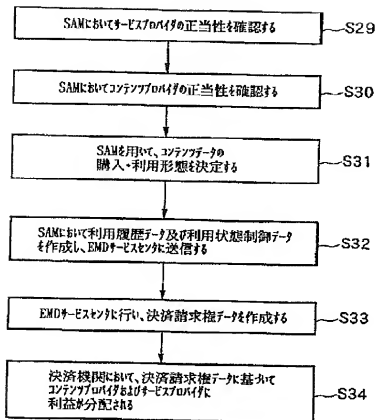
Figure 1 is a block diagram of a system for processing a received signal. The diagram shows the following components and their interconnections:

- Antenna (170):** Receives the signal and outputs to the **Frequency Converter (171)**.
- Frequency Converter (171):** Converts the received signal and outputs to the **Filter (172)**.
- Filter (172):** Filters the signal and outputs to the **Demodulator (173)**.
- Demodulator (173):** Demodulates the signal and outputs to the **Control Unit (182)**.
- Control Unit (182):** Controls the system and outputs to the **Memory (184)** and **Display (186)**.
- Memory (184):** Stores data and outputs to the **Control Unit (182)**.
- Display (186):** Displays information and outputs to the **Control Unit (182)**.
- Power Supply (188):** Provides power to the system and outputs to the **Control Unit (182)**.
- Clock Generator (190):** Generates a clock signal and outputs to the **Control Unit (182)**.

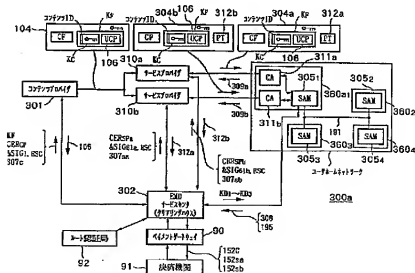
【図 84】



【図85】

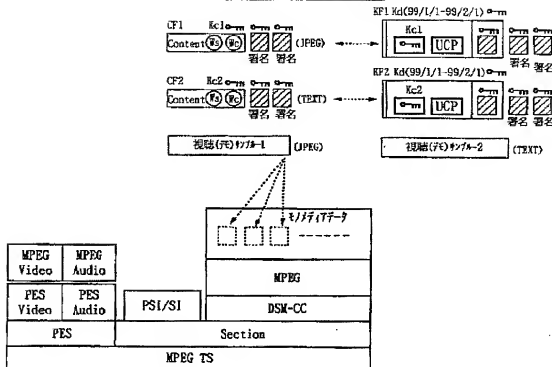


【図97】

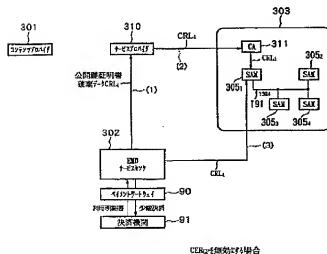


【図93】

デジタル放送のデータ放送方式でMPEGを利用した場合の
プロトコル階層への符号化コンテナの格納

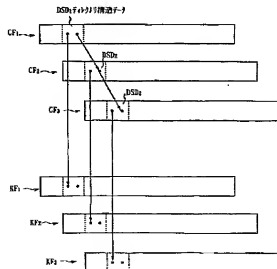


【図102】

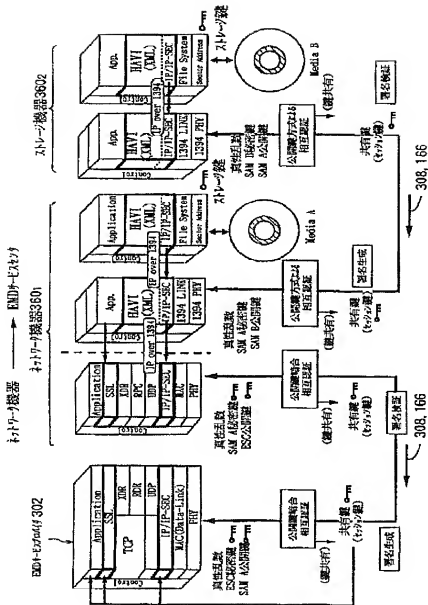


DSM-CCを利用する場合

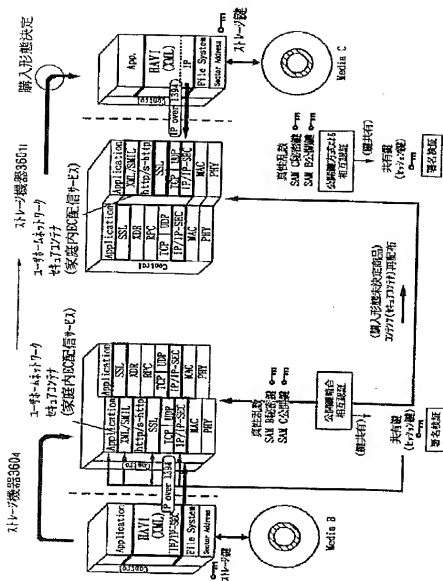
【図112】



【図95】



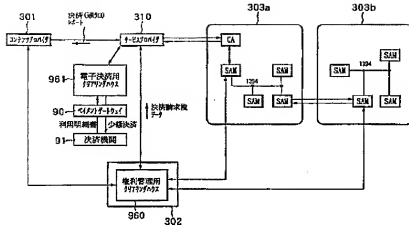
【図 96】



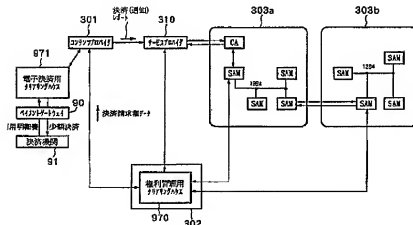
[illegible][illegible]

Figure 1 is a block diagram of a video recording system. The system includes an input source (301) connected to a video compression unit (302). The video compression unit (302) is connected to a video recording unit (310). The video recording unit (310) is connected to a video playback unit (311). The video playback unit (311) is connected to a video output unit (303). The video output unit (303) is connected to a video display unit (303a). The video display unit (303a) is connected to a video output (308). The diagram is labeled with various reference numerals and Japanese text.

【図108】



【図109】



【図115】

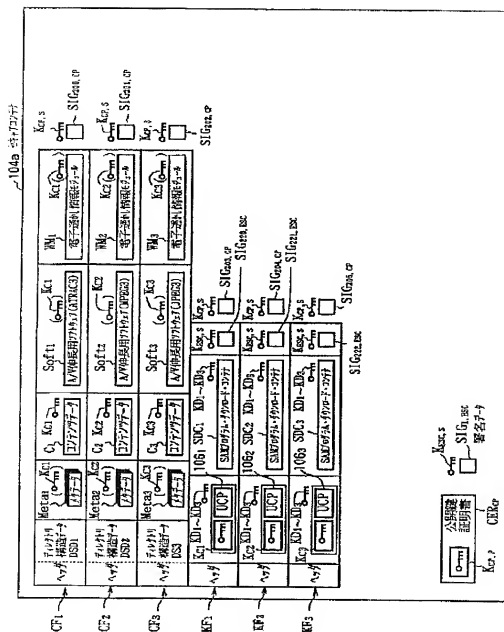
セキュアコンテナ(コンテナ型)のフォーマット①

基本構成

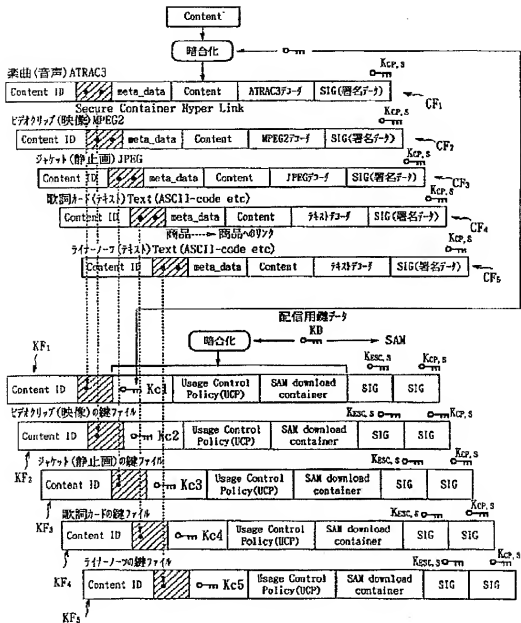
ヘッダ デジタルコンテンツの種類情報 =コンテナ型	サブ エレメント	サブ エレメント	-----	デジタル署名
---------------------------------	-------------	-------------	-------	--------

ヘッダ部	コンテンツID	デジタルコンテンツ	デジタル署名	ヘッダ部	コンテンツID	デジタルコンテンツ	デジタル署名
------	---------	-----------	--------	------	---------	-----------	--------

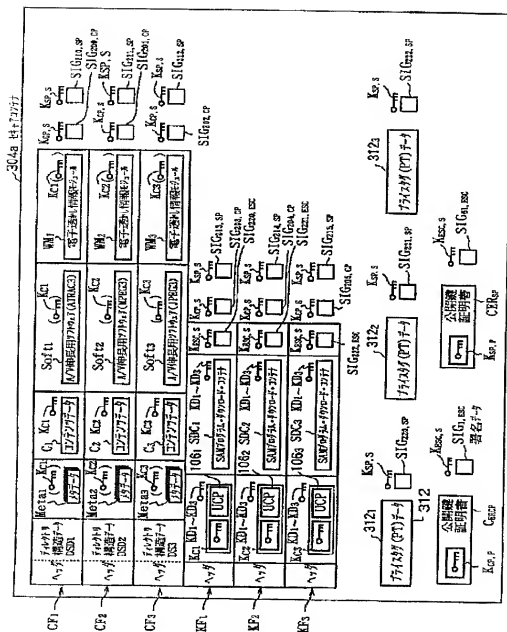
【図 111】



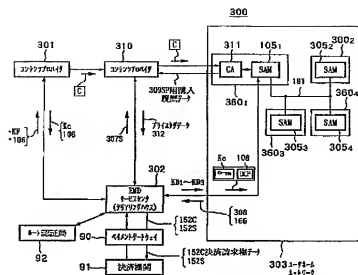
【図113】



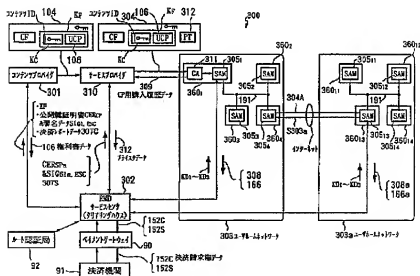
【図 114】



【図125】

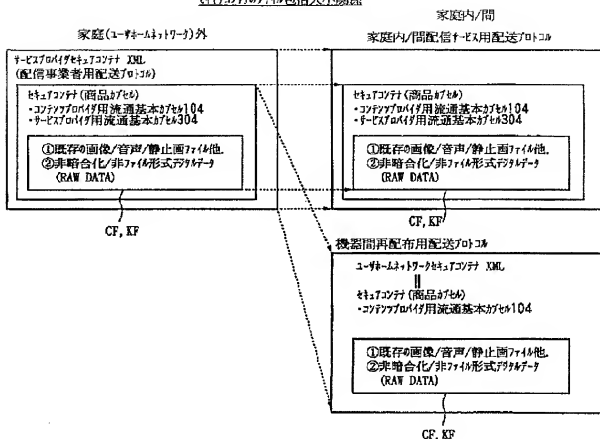


【図126】

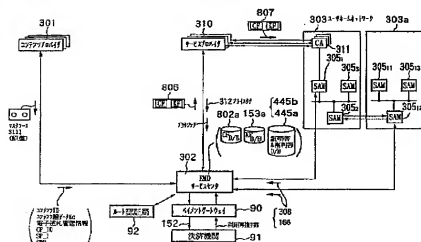


【图 127】

ヒキナリコソ付のワイルド包括大小関係

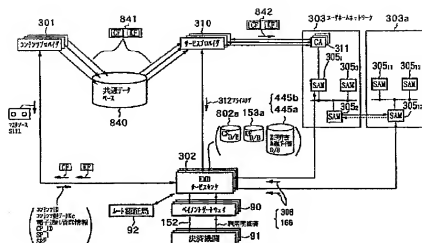


【图 128】

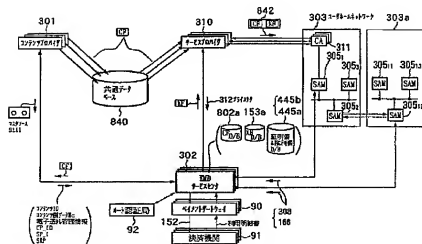


[illegible]

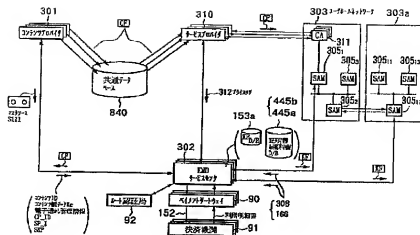
【图 139】



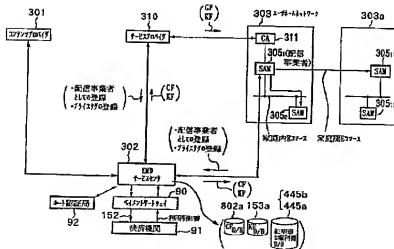
【图 140】



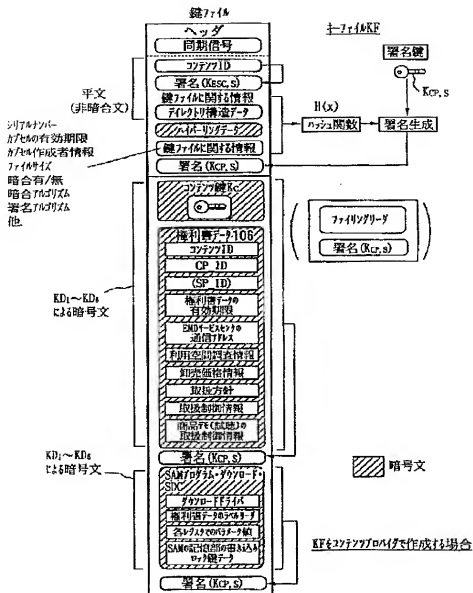
【图 1 4 1】



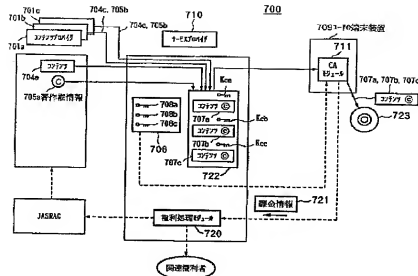
【图 142】



【図 144】



【図145】



【手続補正書】

【提出日】平成12年2月28日(2000.2.28)

【補正対象項目名】全図

【補正方法】変更

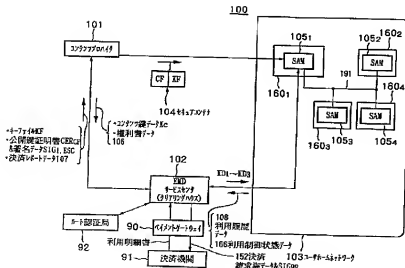
【補正内容】

【手続補正1】

【補正対象書類名】図面

【図1】

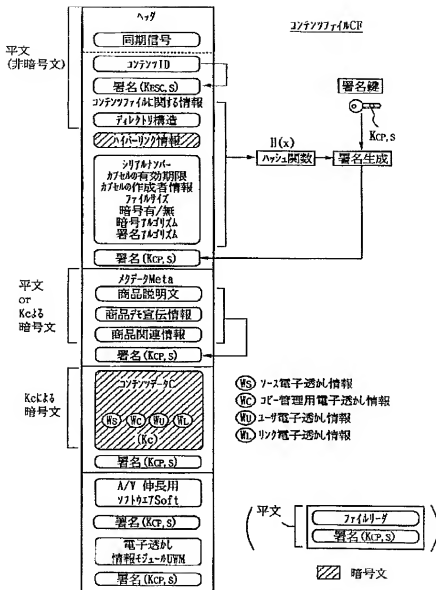
【図27】



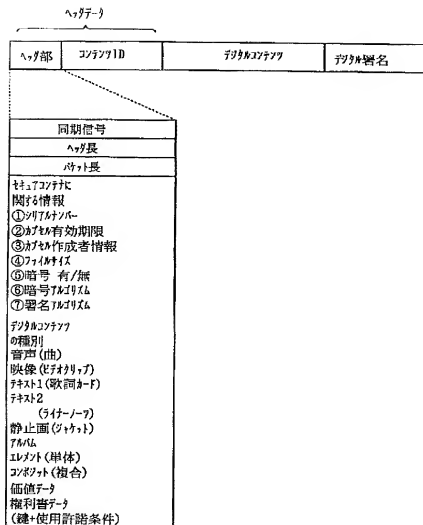
外部メモリに記憶されるデータ

利用履歴データ108
SAM登録リスト

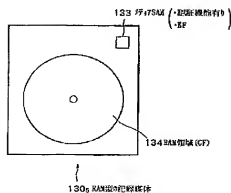
【図6】



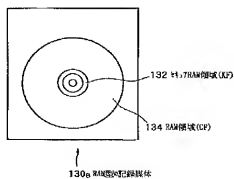
【図 8】



【図 16】

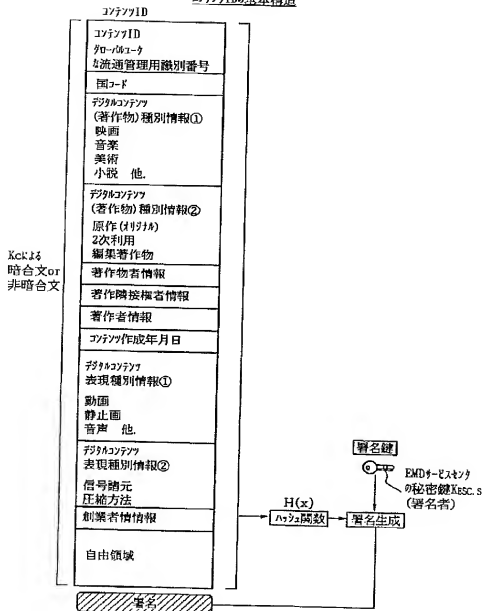


【図 17】



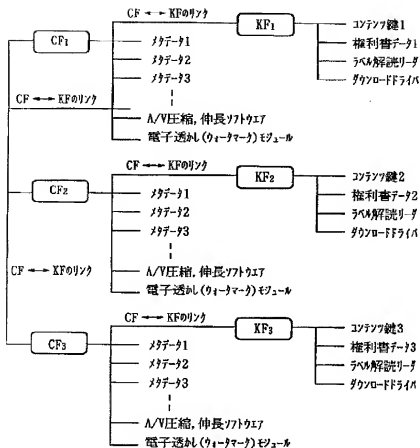
【図 9】

コンテンツIDの基本構造



【図 10】

セキスイコンテナのディレクタリ構造

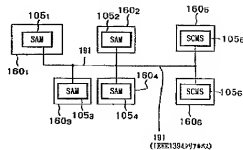


【図 28】

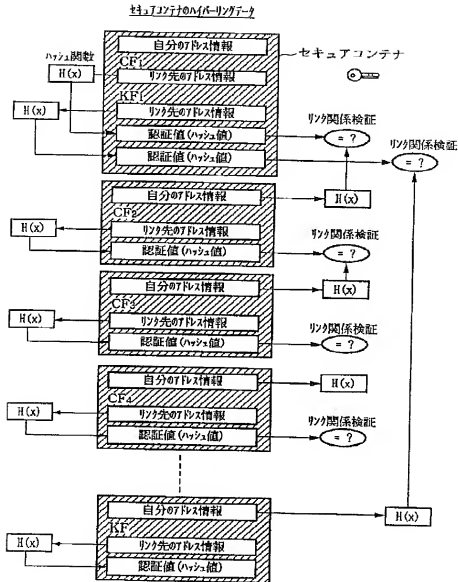
スタックメモリ200k記憶されるデータ

コンテンツ鍵データKc
 権利書データ (UCP) 106
 記憶部 (フラッシュメモリ) 192のロギック鍵データKLoc
 コンテナプロパティ101の公開鍵証明書CERcp
 利用制御情報状態データ (UCS) 166
 SAWプログラム・ダウンロード・コンテナSD1〜SD3

【図 44】



【図 11】

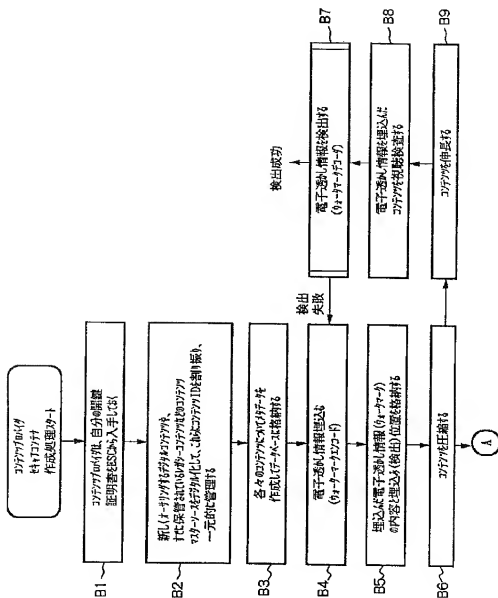



```

graph TD
    Start([コフテアプロバイタからEMD  
サービスへの登録処理スタート]) --> A1[A1: コフテアプロバイタEMDサービスとの  
間で相互認証を行う]
    A1 -- 認証失敗 --> Start
    A1 -- 認証成功 --> A2[A2: セッション鍵を共有する]
    A2 --> A3[A3: 登録を行う権利者データ等とデータ  
ベースが読み付け]
    A3 --> A4[A4: 権利者データに対し、コフテアプロバイタ  
秘密鍵を署名鍵として署名生成を行い、署名を  
含む登録用モジュールを作成]
    A4 --> A5[A5: 登録用モジュールとセッション鍵で暗号化する]
    A5 --> A6[A6: 登録用モジュールとEMDサービス  
センタへ送信する]
    A6 --> A7[A7: EMDサービスから受信した登録要求  
モジュールとセッション鍵で復号化する]
    A7 --> A8[A8: EMDサービスからコフテアプロバイタの公開鍵を署名  
検証鍵として送られてきた登録モジュールに添付されている  
署名データの署名検証を行い、送り主の正当性の  
証明を行う]
    A8 -- 署名検証失敗 --> Stop([登録処理中止])
    A8 -- 署名検証成功 --> A9[A9: 権利者データ等データベースに登録する]
    A9 --> End([登録処理終了])
  
```

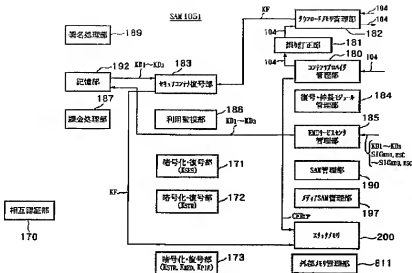
The flowchart illustrates the registration process (登録処理). It begins with a start node (コフテアプロバイタからEMDサービスへの登録処理スタート) leading to step A1 (コフテアプロバイタEMDサービスとの間で相互認証を行う). If authentication fails (認証失敗), it loops back to the start. If successful (認証成功), it proceeds to A2 (セッション鍵を共有する), then A3 (登録を行う権利者データ等とデータベースが読み付け), A4 (権利者データに対し、コフテアプロバイタ秘密鍵を署名鍵として署名生成を行い、署名を含む登録用モジュールを作成), A5 (登録用モジュールとセッション鍵で暗号化する), and A6 (登録用モジュールとEMDサービスセンタへ送信する). Step A7 (EMDサービスから受信した登録要求モジュールとセッション鍵で復号化する) is shown in a dashed box. Step A8 (EMDサービスからコフテアプロバイタの公開鍵を署名検証鍵として送られてきた登録モジュールに添付されている署名データの署名検証を行い、送り主の正当性の証明を行う) is also in a dashed box. If signature verification fails (署名検証失敗), the process ends at 登録処理中止. If successful (署名検証成功), it proceeds to A9 (権利者データ等データベースに登録する) and finally to the end node (登録処理終了).

【図 20】

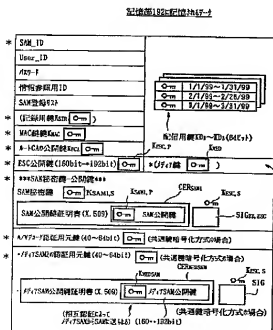


[illegible][illegible][illegible]

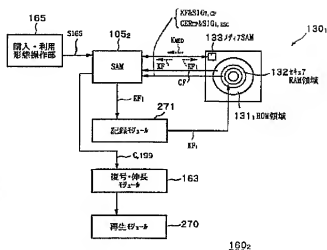
【图 2-6】



【例 30】



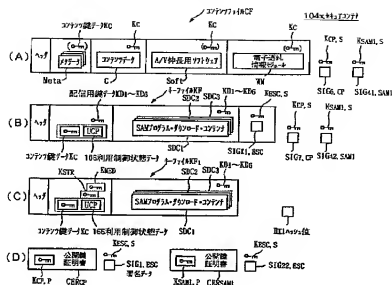
【图 3-6】



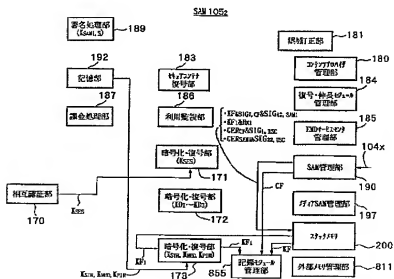
[illegible]

The diagram illustrates the architecture of a 105.1 SAM (Self-Administered Monitoring) system. It features a central processing unit, the 105.1 SAM, which is connected to various input and output modules. The input modules include a Remote Station (189), a Memory (192), a Data Entry (183), and a Data Entry (187). The output modules include a Data Entry (188), a Data Entry (186), a Data Entry (184), a Data Entry (185), a Data Entry (104x), a Data Entry (190), a Data Entry (197), and a Data Entry (200). The system also includes a Data Entry (170) and a Data Entry (171). The 105.1 SAM is connected to a Data Entry (182) and a Data Entry (181). The system is controlled by a Data Entry (170) and a Data Entry (171). The system is connected to a Data Entry (170) and a Data Entry (171). The system is connected to a Data Entry (170) and a Data Entry (171).

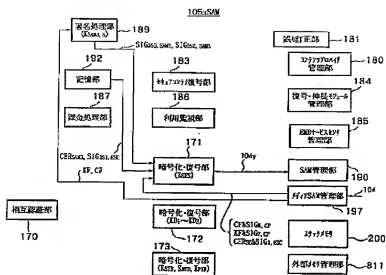
【図34】



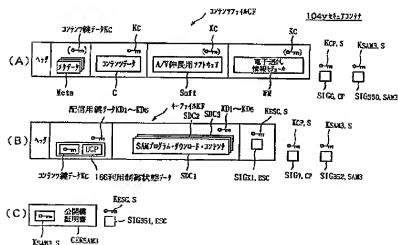
【図35】



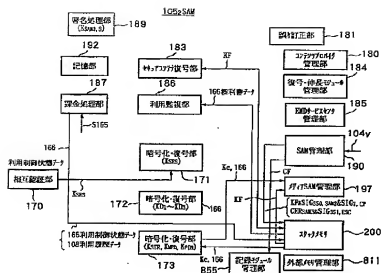
【図 39】



【図 40】

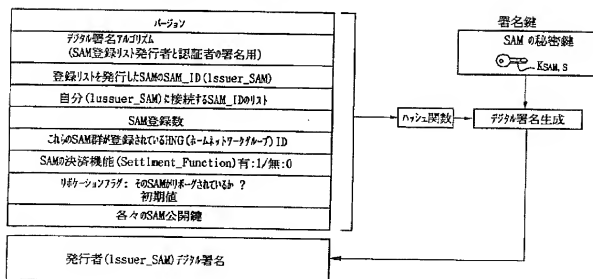


【図 41】

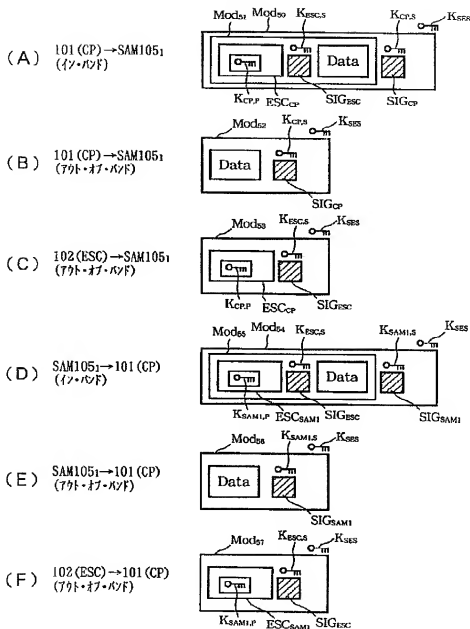


【図 45】

SAM登録リスト (SAM Registration List) (SAM作成)

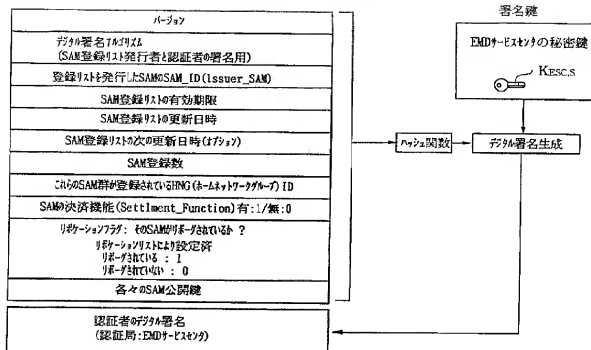


【図 42】

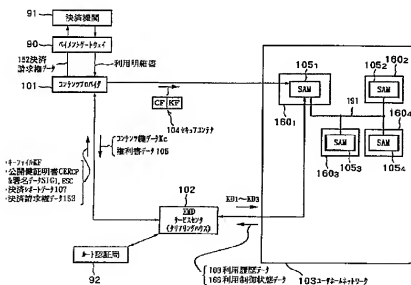


【図 4 6】

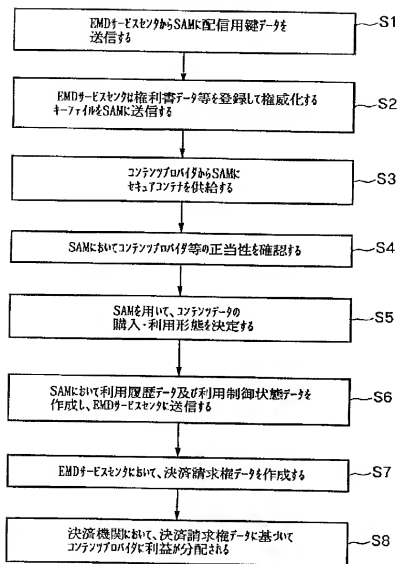
SAM登録リスト (EMDサービス機作成)



【図 4 9】



【図 47】



[illegible]

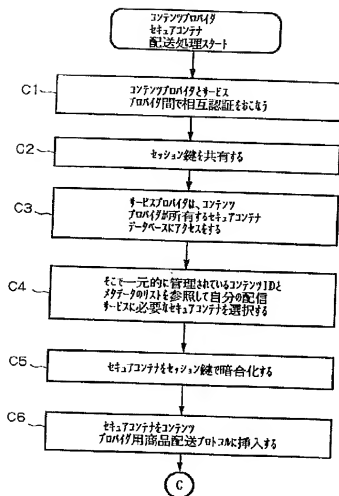
Figure 1 is a block diagram of a data processing system 100. The system includes a host computer 104, a data processing unit 100, a network 102, a database 106, a terminal 102, a printer 104, and a scanner 106. The host computer 104 contains a CPU 106 and memory 108. The data processing unit 100 contains a CPU 106, memory 108, and a data processing unit 100. The network 102 connects the host computer 104 to the data processing unit 100. The database 106 is connected to the data processing unit 100. The terminal 102 is connected to the data processing unit 100. The printer 104 is connected to the data processing unit 100. The scanner 106 is connected to the data processing unit 100. The diagram shows the flow of data between these components.

```

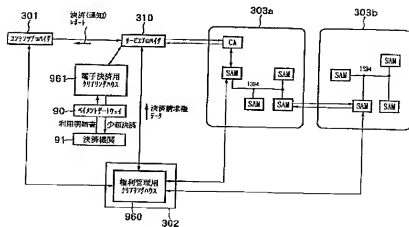
graph TD
    C((C)) --> C7[C7: サービスプロバイダがダウンロードを行う]
    C7 --> C8[C8: コンテンツプロバイダ用商品配送プロトコルからセットアップコンテナを取り出す]
    C8 --> C9[C9: セットアップコンテナをセッション鍵で復号する]
    C9 --> C10[C10: セットアップコンテナ署名検証にも(送り主の正当性)]
    C10 -- "署名検証失敗" --> Stop([受取り中止])
    C10 -- "署名検証成功" --> C11[C11: サービスプロバイダが所有するセットアップコンテナデータベースへ格納する]
    C11 --> End([終了])
  
```

Figure 10 is a flowchart illustrating the signature verification process. It begins with a start node 'C'. The process proceeds to step C7: 'サービスプロバイダがダウンロードを行う' (Service provider performs download). This is followed by step C8: 'コンテンツプロバイダ用商品配送プロトコルからセットアップコンテナを取り出す' (Retrieve setup container from content provider's product delivery protocol). Then, step C9: 'セットアップコンテナをセッション鍵で復号する' (Decrypt setup container with session key). The process then reaches step C10: 'セットアップコンテナ署名検証にも(送り主の正当性)' (Setup container signature verification (sender's legitimacy)). From C10, there are two paths: one for '署名検証失敗' (Signature verification failure) leading to '受取り中止' (Stop receiving), and another for '署名検証成功' (Signature verification success) leading to step C11: 'サービスプロバイダが所有するセットアップコンテナデータベースへ格納する' (Store in setup container database owned by service provider). The process concludes at the '終了' (End) node.

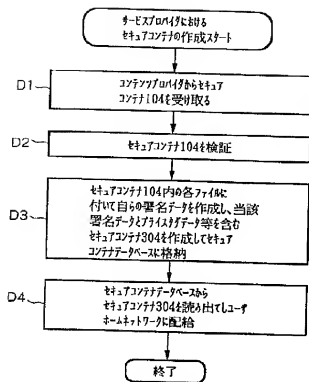
【圖 6 1】



【例】108】



【図 64】

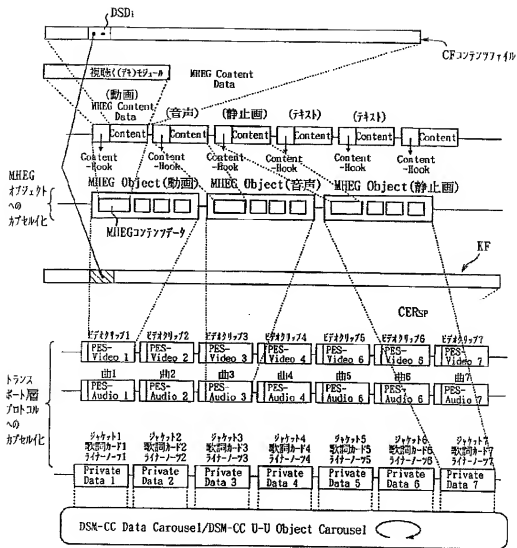


【図 77】

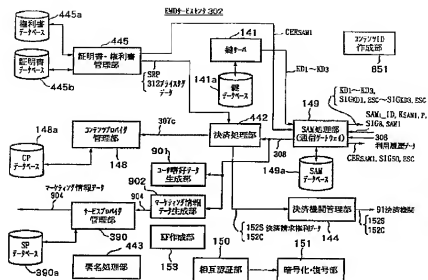
スタックメモリ200の記憶データ

コンテナ鍵データ K_c
 権利書データ (UCP) 106
 不揮発性メモリ201のロック鍵データ K_{Loc}
 コンテナプロバイダ301の公開鍵証明書データ CER_{CP}
 サービスプロバイダ301の公開鍵証明書データ CER_{SP}
 利用制御状態データ (UCS) 166
 SAMプログラム・タスクロード・コンテナ $SD_1 \sim SDC_3$
 プライマリデータ 312

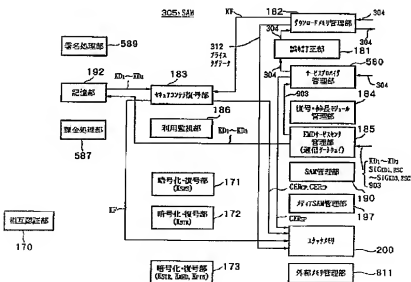
【図66】



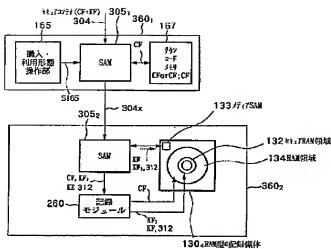
【図72】



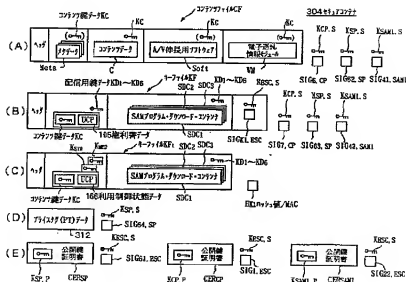
【図76】



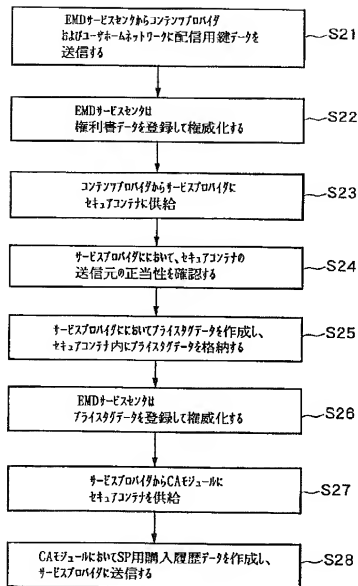
【図80】



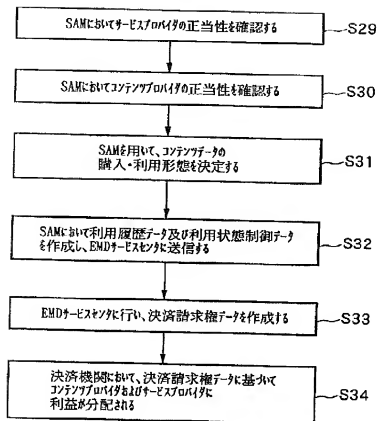
【図81】



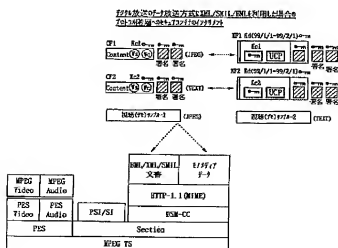
【図84】



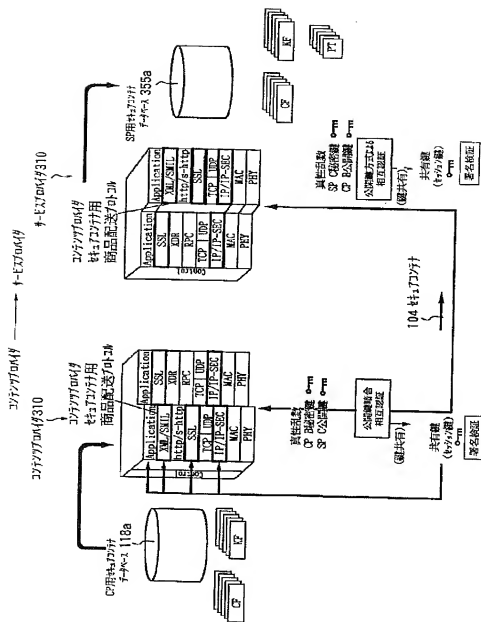
【例 85】



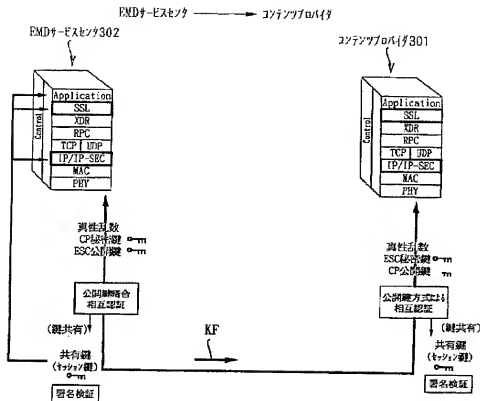
【图 9-2】



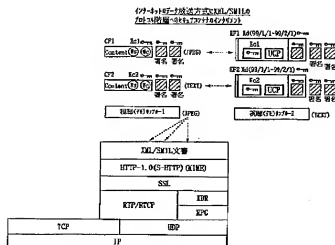
【図 88】



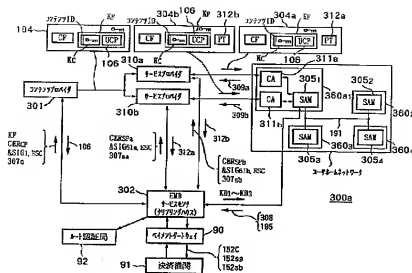
【図 89】



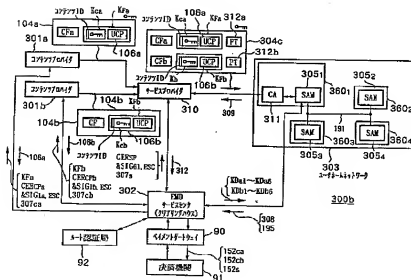
【図 94】



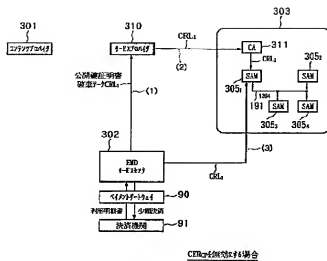
【図 9 7】



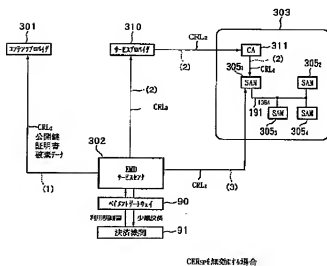
【図 9 8】



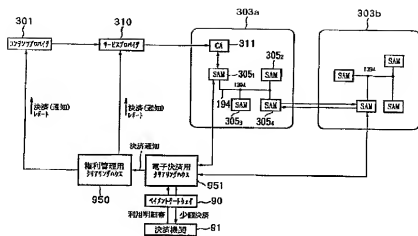
【図 102】



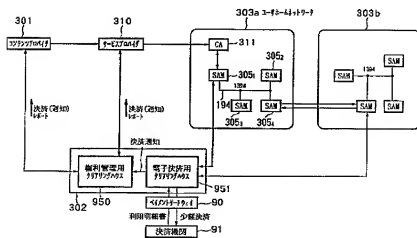
【図 103】



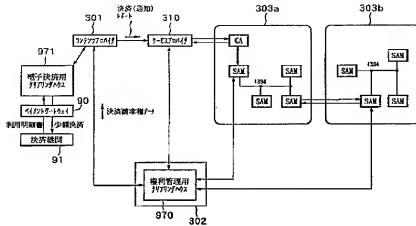
【図106】



【図107】



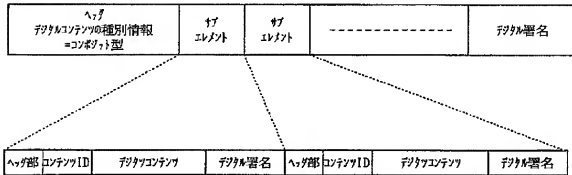
【圖 109】



【圖 1 1 5】

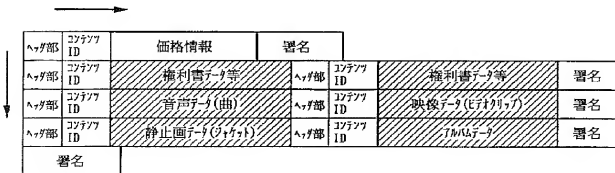
セキアコンテナ(コンポジット型)のデータフォーマット-①

基本構成

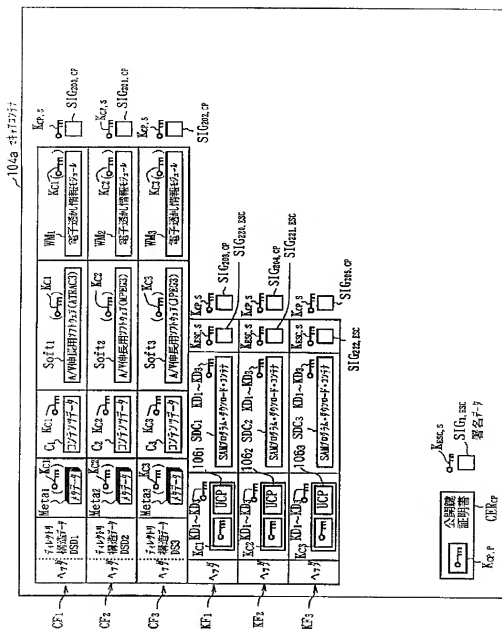


【图 116】

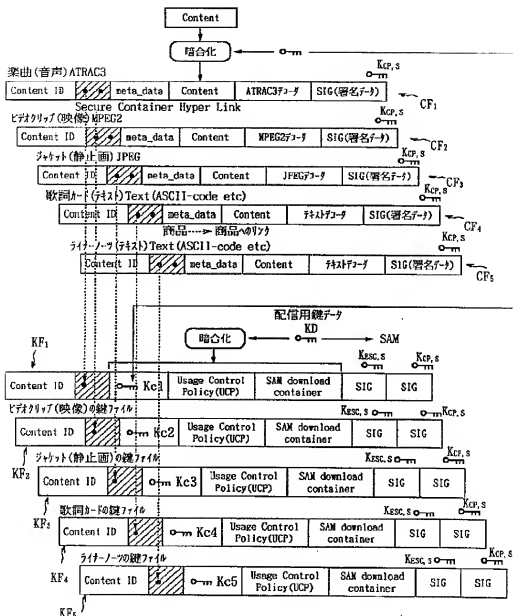
セキアコンテナ(コンボソフト型)のデータフォーマット-②



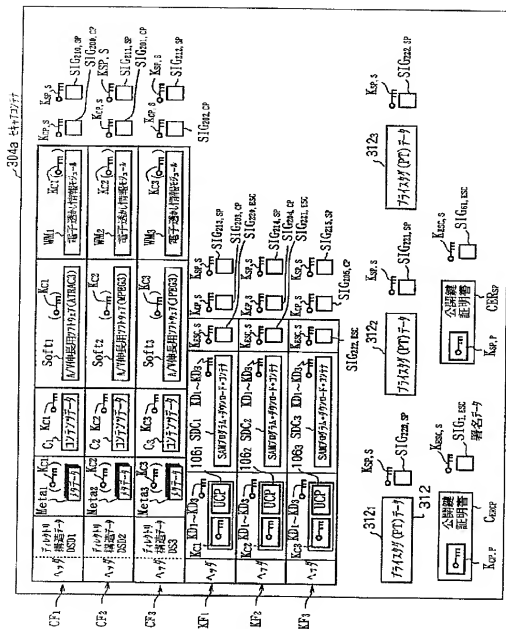
【図 111】



【図113】



【圖 1 1 4】



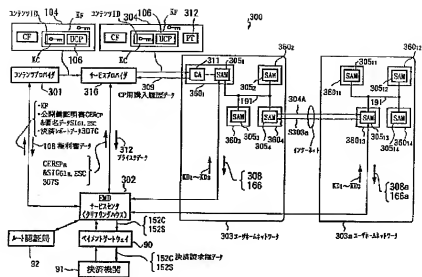
[illegible]

Figure 1 is a block diagram of a video signal processing circuit. The diagram shows a signal flow from input (310) through various stages including a 300SP input stage (311, 1051), a 300SP output stage (302), a 300SP output stage (303), and a 300SP output stage (304). It includes components like a 300SP input stage (311, 1051), a 300SP output stage (302), a 300SP output stage (303), and a 300SP output stage (304). The diagram also shows a 300SP output stage (302) and a 300SP output stage (303).

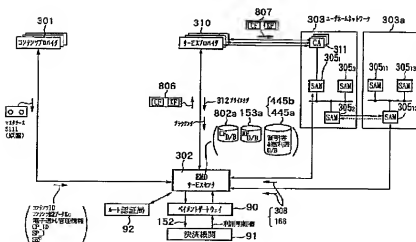
[illegible]

[illegible][illegible]

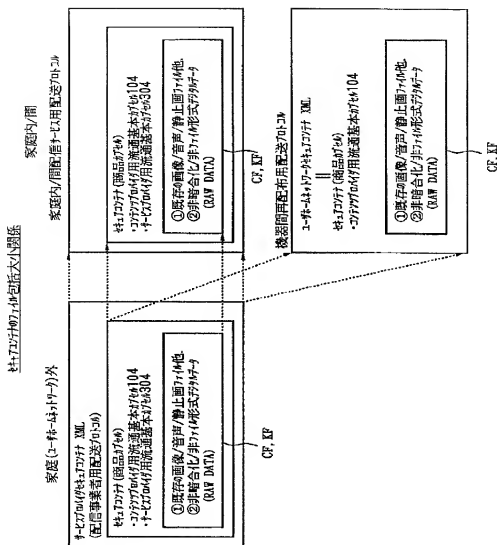
【図126】



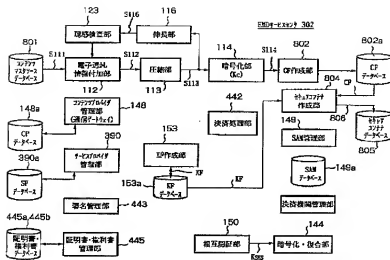
【図128】



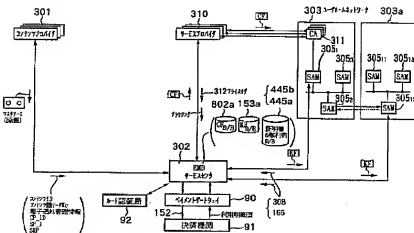
【図127】



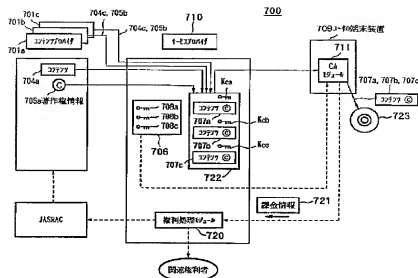
【図129】



【図130】



【図 145】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	7-コード (参考)
G 0 9 C 1/00	6 6 0	G 1 1 B 20/10	H
G 1 1 B 20/10		110 4 L 9/00	6 0 1 C
H 0 4 L 9/32			6 7 5 B
			6 7 5 D

F ターム (参考) 5B017 AA06 BA05 BA07 BB03 BB10
 CA11 CA12 CA16
 5B085 AE13 AE29 B607
 5D044 AB05 DE17 GK17 HL11
 5J104 AA01 AA09 AA16 EA02 EA04
 LA03 LA06 MA02 NA03 PA07
 PA10
 9A001 BB03 BB04 EE02 EE03 EE04
 JJ07 JJ13 LL03

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成18年4月27日(2006.4.27)

【公開番号】特開2001-94549(P2001-94549A)

【公開日】平成13年4月6日(2001.4.6)

【出願番号】特願平11-309721

【国際特許分類】

H 0 4 L	9/08	(2006.01)
G 0 6 F	12/14	(2006.01)
G 0 6 F	21/00	(2006.01)
G 0 9 C	1/00	(2006.01)
G 1 1 B	20/10	(2006.01)
H 0 4 L	9/32	(2006.01)

【F I】

H 0 4 L	9/00	6 0 1 C
G 0 6 F	12/14	3 2 0 B
G 0 6 F	15/00	3 3 0 Z
G 0 9 C	1/00	6 4 0 B
G 0 9 C	1/00	6 4 0 Z
G 0 9 C	1/00	6 6 0 D
G 1 1 B	20/10	11
H 0 4 L	9/00	6 7 5 B
H 0 4 L	9/00	6 7 5 D

【手続補正書】

【提出日】平成18年3月10日(2006.3.10)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項2】

前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを前記キーファイルに付加する

請求項1に記載のデータ提供システム。

【請求項3】

前記データ提供装置は、前記コンテンツデータを格納したコンテンツファイルを作成し

、当該コンテンツファイルを前記データ処理装置に提供する
請求項1に記載のデータ提供システム。

【請求項4】

前記データ提供装置は、前記権利書データを作成して前記管理装置に送り、
前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、
前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項1に記載のデータ提供システム。

【請求項5】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項6】

前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する

請求項5に記載のデータ提供システム。

【請求項7】

前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する

請求項5に記載のデータ提供システム。

【請求項8】

前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項5に記載のデータ提供システム。

【請求項9】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項10】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】削除

【補正の内容】

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】削除

【補正の内容】

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】削除

【補正の内容】

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】削除

【補正の内容】

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】削除

【補正の内容】

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】削除

【補正の内容】

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】削除

【補正の内容】

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】削除
【補正の内容】
【手続補正10】
【補正対象書類名】明細書
【補正対象項目名】0023
【補正方法】削除
【補正の内容】
【手続補正11】
【補正対象書類名】明細書
【補正対象項目名】0024
【補正方法】削除
【補正の内容】
【手続補正12】
【補正対象書類名】明細書
【補正対象項目名】0025
【補正方法】削除
【補正の内容】
【手続補正13】
【補正対象書類名】明細書
【補正対象項目名】0026
【補正方法】削除
【補正の内容】
【手続補正14】
【補正対象書類名】明細書
【補正対象項目名】0027
【補正方法】削除
【補正の内容】
【手続補正15】
【補正対象書類名】明細書
【補正対象項目名】0028
【補正方法】削除
【補正の内容】
【手続補正16】
【補正対象書類名】明細書
【補正対象項目名】0029
【補正方法】削除
【補正の内容】
【手続補正17】
【補正対象書類名】明細書
【補正対象項目名】0030
【補正方法】削除
【補正の内容】
【手続補正18】
【補正対象書類名】明細書
【補正対象項目名】0031
【補正方法】削除
【補正の内容】
【手続補正19】
【補正対象書類名】明細書
【補正対象項目名】0032

【補正方法】削除
【補正の内容】
【手続補正20】
【補正対象書類名】明細書
【補正対象項目名】0033
【補正方法】削除
【補正の内容】
【手続補正21】
【補正対象書類名】明細書
【補正対象項目名】0034
【補正方法】削除
【補正の内容】
【手続補正22】
【補正対象書類名】明細書
【補正対象項目名】0035
【補正方法】削除
【補正の内容】
【手続補正23】
【補正対象書類名】明細書
【補正対象項目名】0036
【補正方法】削除
【補正の内容】
【手続補正24】
【補正対象書類名】明細書
【補正対象項目名】0037
【補正方法】削除
【補正の内容】
【手続補正25】
【補正対象書類名】明細書
【補正対象項目名】0038
【補正方法】削除
【補正の内容】
【手続補正26】
【補正対象書類名】明細書
【補正対象項目名】0039
【補正方法】削除
【補正の内容】
【手続補正27】
【補正対象書類名】明細書
【補正対象項目名】0040
【補正方法】削除
【補正の内容】
【手続補正28】
【補正対象書類名】明細書
【補正対象項目名】0041
【補正方法】削除
【補正の内容】
【手続補正29】
【補正対象書類名】明細書
【補正対象項目名】0042

【補正方法】削除
【補正の内容】
【手続補正30】
【補正対象書類名】明細書
【補正対象項目名】0043
【補正方法】削除
【補正の内容】
【手続補正31】
【補正対象書類名】明細書
【補正対象項目名】0044
【補正方法】削除
【補正の内容】
【手続補正32】
【補正対象書類名】明細書
【補正対象項目名】0045
【補正方法】削除
【補正の内容】
【手続補正33】
【補正対象書類名】明細書
【補正対象項目名】0046
【補正方法】削除
【補正の内容】
【手続補正34】
【補正対象書類名】明細書
【補正対象項目名】0047
【補正方法】削除
【補正の内容】
【手続補正35】
【補正対象書類名】明細書
【補正対象項目名】0048
【補正方法】削除
【補正の内容】
【手続補正36】
【補正対象書類名】明細書
【補正対象項目名】0049
【補正方法】削除
【補正の内容】
【手続補正37】
【補正対象書類名】明細書
【補正対象項目名】0050
【補正方法】削除
【補正の内容】
【手続補正38】
【補正対象書類名】明細書
【補正対象項目名】0051
【補正方法】削除
【補正の内容】
【手続補正39】
【補正対象書類名】明細書
【補正対象項目名】0052

【補正方法】削除
【補正の内容】
【手続補正40】
【補正対象書類名】明細書
【補正対象項目名】00053
【補正方法】削除
【補正の内容】
【手続補正41】
【補正対象書類名】明細書
【補正対象項目名】00054
【補正方法】削除
【補正の内容】
【手続補正42】
【補正対象書類名】明細書
【補正対象項目名】00055
【補正方法】削除
【補正の内容】
【手続補正43】
【補正対象書類名】明細書
【補正対象項目名】00058
【補正方法】削除
【補正の内容】
【手続補正44】
【補正対象書類名】明細書
【補正対象項目名】00059
【補正方法】削除
【補正の内容】
【手続補正45】
【補正対象書類名】明細書
【補正対象項目名】00060
【補正方法】削除
【補正の内容】
【手続補正46】
【補正対象書類名】明細書
【補正対象項目名】00061
【補正方法】削除
【補正の内容】
【手続補正47】
【補正対象書類名】明細書
【補正対象項目名】00062
【補正方法】削除
【補正の内容】
【手続補正48】
【補正対象書類名】明細書
【補正対象項目名】00063
【補正方法】削除
【補正の内容】
【手続補正49】
【補正対象書類名】明細書
【補正対象項目名】00064

【補正方法】 削除
【補正の内容】
【手続補正 5 0】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 6 5
【補正方法】 削除
【補正の内容】
【手続補正 5 1】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 6 6
【補正方法】 削除
【補正の内容】
【手続補正 5 2】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 6 7
【補正方法】 削除
【補正の内容】
【手続補正 5 3】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 6 8
【補正方法】 削除
【補正の内容】
【手続補正 5 4】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 6 9
【補正方法】 削除
【補正の内容】
【手続補正 5 5】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 7 0
【補正方法】 削除
【補正の内容】
【手続補正 5 6】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 7 1
【補正方法】 削除
【補正の内容】
【手続補正 5 7】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 7 2
【補正方法】 削除
【補正の内容】
【手続補正 5 8】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 7 3
【補正方法】 削除
【補正の内容】
【手続補正 5 9】
【補正対象書類名】 明細書
【補正対象項目名】 0 0 7 4

【補正方法】削除
【補正の内容】
【手続補正60】
【補正対象書類名】明細書
【補正対象項目名】0075
【補正方法】削除
【補正の内容】
【手続補正61】
【補正対象書類名】明細書
【補正対象項目名】0076
【補正方法】削除
【補正の内容】
【手続補正62】
【補正対象書類名】明細書
【補正対象項目名】0077
【補正方法】削除
【補正の内容】
【手続補正63】
【補正対象書類名】明細書
【補正対象項目名】0078
【補正方法】削除
【補正の内容】
【手続補正64】
【補正対象書類名】明細書
【補正対象項目名】0079
【補正方法】削除
【補正の内容】
【手続補正65】
【補正対象書類名】明細書
【補正対象項目名】0080
【補正方法】削除
【補正の内容】
【手続補正66】
【補正対象書類名】明細書
【補正対象項目名】0081
【補正方法】削除
【補正の内容】
【手続補正67】
【補正対象書類名】明細書
【補正対象項目名】0082
【補正方法】削除
【補正の内容】
【手続補正68】
【補正対象書類名】明細書
【補正対象項目名】0083
【補正方法】削除
【補正の内容】
【手続補正69】
【補正対象書類名】明細書
【補正対象項目名】0084

【補正方法】削除

【補正の内容】

【手続補正70】

【補正対象書類名】明細書

【補正対象項目名】0085

【補正方法】削除

【補正の内容】

【手続補正71】

【補正対象書類名】明細書

【補正対象項目名】0086

【補正方法】削除

【補正の内容】

【手続補正72】

【補正対象書類名】明細書

【補正対象項目名】0087

【補正方法】削除

【補正の内容】

【手続補正73】

【補正対象書類名】明細書

【補正対象項目名】0088

【補正方法】削除

【補正の内容】